

Dell PowerConnect
6200 Series System

CLI Reference Guide

**Regulatory Models: PC6224, PC6248,
PC6224P, PC6248P, and PC6224F**



Notes



NOTE: A NOTE indicates important information that helps you make better use of your computer.

Information in this publication is subject to change without notice.

© 2011 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, PowerConnect™, OpenManage™ are trademarks of Dell Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. sFlow® is a registered trademark of InMon Corporation. Cisco® is a registered trademark of Cisco Systems.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Regulatory Models: PC6224, PC6248, PC6224P, PC6248P, and PC6224F

March 2011

Rev. A06

Contents

1	Command Groups	59
	Introduction	59
	Command Groups	59
	Mode Types	64
	Layer 2 Commands	65
	Layer 3 Commands	94
	Utility Commands	120
2	Using the CLI	139
	Introduction	139
	Entering and Editing CLI Commands	139
	CLI Command Modes	145
	Starting the CLI	158
	Using CLI Functions and Tools	169
3	AAA Commands	191
	aaa authentication dot1x	192
	aaa authentication enable	193

aaa authentication login	194
aaa authorization network default radius.	196
enable authentication	197
enable password.	198
ip http authentication	199
ip https authentication.	200
login authentication	201
password (Line Configuration).	202
password (User EXEC).	202
show authentication methods	203
show users accounts	205
show users login-history	206
username.	207
 4 ACL Commands	 209
access-list	210
deny permit	211
ip access-group	213
no ip access-group.	213
mac access-group	214
mac access-list extended	216
mac access-list extended rename	217

show ip access-lists	218
show mac access-list	219
5 Address Table Commands	221
bridge address	222
bridge aging-time	223
bridge multicast address	223
bridge multicast filtering	225
bridge multicast forbidden address	226
bridge multicast forbidden forward-unregistered	227
bridge multicast forward-all	228
bridge multicast forward-unregistered	228
clear bridge	229
port security	230
port security max	231
show bridge address-table	232
show bridge address-table count	233
show bridge address-table static	234
show bridge multicast address-table	235
show bridge multicast filtering	236
show ports security	237
show ports security addresses	238

6	CDP Interoperability Commands	241
	clear isdp counters	242
	clear isdp table.	242
	isdp advertise-v2.	243
	isdp enable.	243
	isdp holdtime.	244
	isdp timer.	245
	show isdp	246
	show isdp entry	247
	show isdp interface	249
	show isdp neighbors.	251
	show isdp traffic	252
7	DHCP Layer 2 Relay Commands.	255
	dhcp l2relay (Global Configuration)	256
	dhcp l2relay (Interface Configuration).	256
	dhcp l2relay circuit-id	257
	dhcp l2relay remote-id.	258
	dhcp l2relay trust.	259
	dhcp l2relay vlan	259

8	DHCP Snooping Commands	261
	clear ip dhcp snooping statistics	262
	ip dhcp snooping	262
	ip dhcp snooping binding	263
	ip dhcp snooping database	264
	ip dhcp snooping database write-delay	265
	ip dhcp snooping limit	266
	ip dhcp snooping log-invalid	267
	ip dhcp snooping trust	267
	ip dhcp snooping verify mac-address	268
	show ip dhcp snooping	269
	show ip dhcp snooping binding	270
	show ip dhcp snooping database	271
	show ip dhcp snooping interfaces	272
	show ip dhcp snooping statistics	273
9	Dynamic ARP Inspection Commands	275
	arp access-list	276
	clear counters ip arp inspection	276
	ip arp inspection filter	277
	ip arp inspection limit	278

ip arp inspection trust	279
ip arp inspection validate	280
ip arp inspection vlan	281
permit ip host mac host	282
show arp access-list.	282
show ip arp inspection ethernet.	283
show ip arp inspection statistics	285
show ip arp inspection vlan	287

10 Ethernet Configuration Commands 289

clear counters	290
description	290
duplex	291
flowcontrol.	292
interface ethernet	293
interface range ethernet.	293
mtu	294
negotiation	295
show interfaces advertise.	296
show interfaces configuration.	297
show interfaces counters	299
show interfaces description.	302

show interfaces detail	303
show interfaces status	307
show statistics ethernet	310
show storm-control	314
shutdown	316
speed	316
storm-control broadcast	317
storm-control multicast	318
storm-control unicast	319
 11 GVRP Commands	 321
clear gvrp statistics	322
garp timer	322
gvrp enable (global)	324
gvrp enable (interface)	324
gvrp registration-forbid	325
gvrp vlan-creation-forbid	326
show gvrp configuration	327
show gvrp error-statistics	328
show gvrp statistics	330

12 IGMP Snooping Commands 333

ip igmp snooping (global)	334
ip igmp snooping (interface)	334
ip igmp snooping host-time-out	335
ip igmp snooping leave-time-out	336
ip igmp snooping mrouter-time-out	337
show ip igmp snooping groups	338
show ip igmp snooping interface	339
show ip igmp snooping mrouter	340
ip igmp snooping (VLAN)	341
ip igmp snooping fast-leave	341
ip igmp snooping groupmembership-interval	342
ip igmp snooping maxresponse	343
ip igmp snooping mcrtrexpiretime	344

13 IGMP Snooping Querier Commands . . . 347

ip igmp snooping querier	348
ip igmp snooping querier election participate	349
ip igmp snooping querier query-interval	350
ip igmp snooping querier timer expiry	351

ip igmp snooping querier version	351
show igmp snooping querier	352
14 IP Addressing Commands	355
clear host	356
ip address	356
ip address dhcp	357
ip address vlan.	358
ip default-gateway.	359
ip domain-lookup	360
ip domain-name	360
ip host	361
ip name-server.	362
ipv6 address	363
ipv6 enable.	364
ipv6 gateway.	365
show arp switch	366
show hosts	367
show ip helper-address	368
show ip interface management	369

15 IPv6 Access List Commands	371
{deny permit}	372
ipv6 access-list	374
ipv6 access-list rename	375
ipv6 traffic-filter	376
show ipv6 access-lists.	377
16 IPv6 MLD Snooping Querier Commands	381
ipv6 mld snooping querier	382
ipv6 mld snooping querier (VLAN mode)	382
ipv6 mld snooping querier address	383
ipv6 mld snooping querier election participate.	384
ipv6 mld snooping querier query-interval	385
ipv6 mld snooping querier timer expiry	385
show ipv6 mld snooping querier.	386
17 iSCSI Optimization Commands.	389
iscsi enable	390
show iscsi	391

18 LACP Commands	393
lacp port-priority	394
lacp system-priority	394
lacp timeout	395
show lacp ethernet	396
show lacp port-channel	398
19 Link Dependency Commands	401
link-dependency group	402
no link-dependency group	402
add ethernet	403
add port-channel	404
no add port-channel	404
depends-on ethernet	405
no depends-on ethernet	406
depends-on port-channel	406
no depends-on port-channel	407
show link-dependency	408
20 LLDP Commands	411
clear lldp remote-data	412
clear lldp statistics	412

lldp med	413
lldp med confignotification	414
lldp med faststartrepeatcount	414
lldp med transmit-tlv	415
lldp notification	416
lldp notification-interval	417
lldp receive	418
lldp timers	418
lldp transmit	420
lldp transmit-mgmt	420
lldp transmit-tlv	421
show lldp	422
show lldp interface	423
show lldp local-device	424
show lldp med	426
show lldp med interface	426
show lldp med local-device	428
show lldp med remote-device	430
show lldp remote-device	433
show lldp statistics	435

21	Port Channel Commands	439
	channel-group	440
	interface port-channel	441
	interface range port-channel	441
	hashing-mode	442
	no hashing-mode	443
	show interfaces port-channel	444
	show statistics port-channel	445
22	Port Monitor Commands	449
	monitor session	450
	show monitor session	451
23	QoS Commands	453
	assign-queue	455
	class	455
	class-map	456
	class-map rename	457
	classofservice dot1p-mapping	458
	classofservice ip-dscp-mapping	459
	classofservice trust	460
	conform-color	461

cos-queue min-bandwidth	461
cos-queue strict	462
diffserv	463
drop.	464
mark cos	465
mark ip-dscp	465
mark ip-precedence	466
match class-map	467
match cos	468
match destination-address mac	469
match dstip	470
match dstip6	471
match dstl4port.	471
match ethertype	472
match ip6flowlbl	473
match ip dscp	474
match ip precedence.	475
match ip tos	475
match protocol	476
match source-address mac	477
match srcip.	478

match srcip6	479
match srcI4port	480
match vlan	481
mirror.	481
police-simple	482
policy-map	483
redirect.	484
service-policy	485
show class-map	486
show classofservice dot1p-mapping	488
show classofservice ip-dscp-mapping	490
show classofservice trust	493
show diffserv.	494
show diffserv service interface ethernet in.	495
show diffserv service interface port-channel in	496
show diffserv service brief	497
show interfaces cos-queue	498
show policy-map	500
show policy-map interface	501
show service-policy	502
traffic-shape	504

24 RADIUS Commands	505
aaa accounting network default start-stop	
group radius	506
acct-port	506
auth-port	507
deadtime	508
key	509
msgauth	509
name	510
primary	511
priority	511
radius-server deadtime	512
radius-server host	513
radius-server key	514
radius-server retransmit	515
radius-server source-ip	515
radius-server timeout	516
retransmit	517
show radius-servers	518
show radius-servers statistics	521

source-ip	525
timeout	525
usage	526
 25 Spanning Tree Commands	 529
clear spanning-tree detected-protocols	531
exit (mst)	531
instance (mst)	532
name (mst)	533
revision (mst)	534
show spanning-tree	534
show spanning-tree summary	542
spanning-tree	544
spanning-tree auto-portfast	545
spanning-tree bpdu flooding	545
spanning-tree bpdu-protection	546
spanning-tree cost	547
spanning-tree disable	548
spanning-tree forward-time	549
spanning-tree guard	550
spanning-tree loopguard	550
spanning-tree max-age	551

spanning-tree max-hops	552
spanning-tree mode	553
spanning-tree mst 0 external-cost.	553
spanning-tree mst configuration	554
spanning-tree mst cost.	555
spanning-tree mst port-priority	556
spanning-tree mst priority	557
spanning-tree portfast	558
spanning-tree portfast bpdupfilter default	559
spanning-tree portfast default	560
spanning-tree port-priority	560
spanning-tree priority	561
spanning-tree tcnguard	562
spanning-tree transmit hold-count	563
 26 Switchport Voice Commands	 565
show switchport voice.	566
switchport voice detect auto	568
 27 TACACS+ Commands	 569
key	570
port	570

priority	571
show tacacs	572
tacacs-server host	573
tacacs-server key	573
tacacs-server timeout	574
timeout	575
 28 VLAN Commands	 577
dvlan-tunnel ethertype.	579
interface vlan	579
interface range vlan	580
mode dvlan-tunnel	581
name	582
protocol group	583
protocol vlan group	584
protocol vlan group all.	585
show dvlan-tunnel	586
show dvlan-tunnel interface	586
show interfaces switchport	587
show port protocol.	591
show switchport protected	592
show vlan	593

show vlan association mac	594
show vlan association subnet	595
switchport access vlan	596
switchport forbidden vlan	596
switchport general acceptable-frame-type tagged-only.	597
switchport general allowed vlan	598
switchport general ingress-filtering disable	599
switchport general pvid	600
switchport mode	601
switchport protected.	602
switchport protected name	603
switchport trunk allowed vlan.	604
vlan	604
vlan association mac	605
vlan association subnet	606
vlan database	607
vlan makestatic	608
vlan protocol group	608
vlan protocol group add protocol	609
vlan protocol group name	611

vlan protocol group remove	612
vlan routing	613
29 Voice VLAN Commands	615
voice vlan	616
voice vlan (Interface)	616
voice vlan data priority	617
show voice vlan	618
30 802.1x Commands	621
dot1x mac-auth-bypass	622
dot1x max-req	622
dot1x max-users	623
dot1x port-control	624
dot1x re-authenticate	625
dot1x re-authentication	626
dot1x system-auth-control.	627
dot1x timeout guest-vlan-period	627
dot1x timeout quiet-period	628
dot1x timeout re-authperiod.	629
dot1x timeout server-timeout	630
dot1x timeout supp-timeout	631

dot1x timeout tx-period	632
show dot1x	633
show dot1x clients	636
show dot1x ethernet	638
show dot1x statistics	640
show dot1x users	642
dot1x guest-vlan	643
dot1x unauth-vlan	644
show dot1x advanced	645
radius-server attribute 4	647
 31 ARP Commands	 649
arp	650
arp cachesize	650
arp dynamicrenew	651
arp purge	652
arp resptime	653
arp retries	654
arp timeout	655
clear arp-cache	655
clear arp-cache management	656

ip proxy-arp	657
show arp	657
32 DHCP and BOOTP Relay Commands . . .	659
bootpdhcprelay cidridoptmode	660
bootpdhcprelay maxhopcount.	661
bootpdhcprelay minwaittime	661
bootpdhcprelay cidridoptmode	662
show bootpdhcprelay	663
33 DHCPv6 Commands	665
clear ipv6 dhcp.	666
dns-server	666
domain-name	667
ipv6 dhcp pool	668
ipv6 dhcp relay.	669
ipv6 dhcp relay-agent-info-opt	670
ipv6 dhcp relay-agent-info-remote-id-subopt.	671
ipv6 dhcp server	671
prefix-delegation	672
service dhcpv6.	673
show ipv6 dhcp	674

show ipv6 dhcp binding	675
show ipv6 dhcp interface	676
show ipv6 dhcp pool	678
show ipv6 dhcp statistics	678
 34 DVMRP Commands	 681
ip dvmrp	682
ip dvmrp metric.	682
ip dvmrp trapflags	683
show ip dvmrp	684
show ip dvmrp interface	685
show ip dvmrp neighbor	685
show ip dvmrp nexthop	686
show ip dvmrp prune.	687
show ip dvmrp route	688
 35 IGMP Commands	 689
ip igmp	690
ip igmp last-member-query-count.	690
ip igmp last-member-query-interval.	691
ip igmp query-interval	692
ip igmp query-max-response-time	693

ip igmp robustness.	694
ip igmp startup-query-count.	694
ip igmp startup-query-interval.	695
ip igmp version.	696
show ip igmp.	697
show ip igmp groups.	698
show ip igmp interface	699
show ip igmp interface membership	700
show ip igmp interface stats	701
 36 IGMP Proxy Commands	 703
ip igmp-proxy	704
ip igmp-proxy reset-status	704
ip igmp-proxy unsolicited-report-interval	705
show ip igmp-proxy	706
show ip igmp-proxy interface	707
show ip igmp-proxy groups	708
show ip igmp-proxy groups detail	709

37 IP Helper Commands	711
clear ip helper statistics	712
ip helper-address (global configuration)	712
ip helper-address (interface configuration).	714
ip helper enable	716
show ip helper-address	717
show ip helper statistics.	718
 38 IP Routing Commands	 721
encapsulation	722
ip address	722
ip mtu	723
ip netdirbcast.	724
ip route	725
ip route default	726
ip route distance	727
ip routing	728
routing	729
show ip brief	730
show ip interface	730
show ip protocols	732

show ip route	734
show ip route preferences	735
show ip route summary	736
show ip stats	737
vlan routing	739
 39 IPv6 MLD Snooping Commands	 741
ipv6 mld snooping immediate-leave	742
ipv6 mld snooping groupmembership-interval	743
ipv6 mld snooping maxresponse	743
ipv6 mld snooping mcrtexpiretime	744
ipv6 mld snooping (Global)	745
ipv6 mld snooping (Interface)	746
ipv6 mld snooping (VLAN)	746
show ipv6 mld snooping	747
show ipv6 mld snooping groups	749
 40 IPv6 Multicast Commands	 751
ipv6 pimsm (Global config)	752
ipv6 pimsm (VLAN Interface config)	752
ipv6 pimsm bsr-border	753
ipv6 pimsm bsr-candidate	754

ipv6 pimsm dr-priority	755
ipv6 pimsm hello-interval	755
ipv6 pimsm join-prune-interval	756
ipv6 pimsm register-threshold	757
ipv6 pimsm rp-address.	757
ipv6 pimsm rp-candidate.	758
ipv6 pimsm spt-threshold	759
ipv6 pimsm ssm	760
show ipv6 pimsm.	760
show ipv6 pimsm bsr.	762
show ipv6 pimsm interface	763
show ipv6 pimsm neighbor	764
show ipv6 pimsm rphash.	765
show ipv6 pimsm rp mapping	765

41 IPv6 Routing Commands 767

clear ipv6 neighbors	769
clear ipv6 statistics	769
ipv6 address	770
ipv6 enable	771
ipv6 forwarding	772
ipv6 host	773

ipv6 mld last-member-query-count	774
ipv6 mld last-member-query-interval	774
ipv6 mld-proxy	775
ipv6 mld-proxy reset-status	776
ipv6 mld-proxy unsolicit-rprt-interval.	776
ipv6 mld query-interval	777
ipv6 mld query-max-response-time	778
ipv6 mld router	779
ipv6 mtu	779
ipv6 nd dad attempts.	780
ipv6 nd managed-config-flag	781
ipv6 nd ns-interval	782
ipv6 nd other-config-flag	783
ipv6 nd prefix.	784
ipv6 nd ra-interval	785
ipv6 nd ra-lifetime	786
ipv6 nd reachable-time	787
ipv6 nd suppress-ra	788
ipv6 pimdm	788
ipv6 pimdm hello-interval	789
ipv6 route.	790

ipv6 route distance	791
ipv6 unicast-routing	792
ping ipv6	792
ping ipv6 interface	793
show ipv6 brief	795
show ipv6 interface	795
show ipv6 mld groups	797
show ipv6 mld interface	800
show ipv6 mld-proxy	803
show ipv6 mld-proxy groups	804
show ipv6 mld-proxy groups detail	805
show ipv6 mld-proxy interface	808
show ipv6 mld traffic	809
show ipv6 neighbors	810
show ipv6 pimdm	811
show ipv6 pimdm interface	812
show ipv6 pimdm neighbor	813
show ipv6 route	814
show ipv6 route preferences	815
show ipv6 route summary	816
show ipv6 traffic	817

show ipv6 vlan	819
traceroute ipv6	820
42 Loopback Interface Commands	823
interface loopback	824
show interfaces loopback	824
43 Multicast Commands	827
ip mcast boundary	829
ip mroute	829
ip multicast	830
ip multicast ttl-threshold	831
ip pimsm	832
ip pimsm bsr-border	833
ip pimsm bsr-candidate	833
ip pimsm dr-priority	834
ip pimsm hello-interval	835
ip pimsm join-prune-interval	836
ip pimsm register-threshold	836
ip pimsm rp-address	837
ip pimsm rp-candidate	838
ip pimsm spt-threshold	839

ip pimsm ssm	839
show bridge multicast address-table count	840
show ip mcast	841
show ip mcast boundary	842
show ip mcast interface	843
show ip mcast mroute	844
show ip mcast mroute group	845
show ip mcast mroute source	846
show ip mcast mroute static	847
show ip pimsm bsr	848
show ip pimsm interface	849
show ip pimsm rhash	850
show ip pimsm rp mapping	851
 44 OSPF Commands	 853
area default-cost	856
area nssa	856
area nssa default-info-originate	857
area nssa no-redistribute	858
area nssa no-summary	859
area nssa translator-role	860
area nssa translator-stab-intv	860

area range	861
area stub	862
area stub no-summary	863
area virtual-link	864
area virtual-link authentication	865
area virtual-link dead-interval	866
area virtual-link hello-interval	867
area virtual-link retransmit-interval	868
area virtual-link transmit-delay	869
auto-cost	870
bandwidth	871
capability opaque	871
clear ip ospf	872
default-information originate	873
default-metric	874
distance ospf	875
distribute-list out	876
enable	877
exit-overflow-interval	877
external-lsdb-limit	878
ip ospf area	879

ip ospf authentication	880
ip ospf cost	881
ip ospf dead-interval	881
ip ospf hello-interval	882
ip ospf mtu-ignore	883
ip ospf network.	884
ip ospf priority	885
ip ospf retransmit-interval	886
ip ospf transmit-delay	886
maximum-paths	887
network area	888
nsf	889
nsf helper.	890
nsf helper strict-lsa-checking	891
nsf restart-interval	892
passive-interface default	893
passive-interface	894
redistribute	894
router-id	896
router ospf	896
show ip ospf	897

show ip ospf abr	903
show ip ospf area	903
show ip ospf asbr	905
show ip ospf database.	906
show ip ospf database database-summary	909
show ip ospf interface.	911
show ip ospf interface brief	913
show ip ospf interface stats	913
show ip ospf neighbor	914
show ip ospf range.	918
show ip ospf statistics.	918
show ip ospf stub table	919
show ip ospf virtual-link.	920
show ip ospf virtual-link brief.	921
timers spf.	922
1583compatibility	923
 45 OSPFv3 Commands	 925
area default-cost.	928
area nssa.	928
area nssa default-info-originate	929
area nssa no-redistribute	930

area nssa no-summary	931
area nssa translator-role	932
area nssa translator-stab-intv	933
area range	934
area stub	935
area stub no-summary	936
area virtual-link	936
area virtual-link dead-interval	937
area virtual-link hello-interval	938
area virtual-link retransmit-interval	939
area virtual-link transmit-delay	940
default-information originate	941
default-metric	942
distance ospf	942
enable	943
exit-overflow-interval	944
external-lsdb-limit	945
ipv6 ospf	946
ipv6 ospf areaid	946
ipv6 ospf cost	947
ipv6 ospf dead-interval	948

ipv6 ospf hello-interval	949
ipv6 ospf mtu-ignore	950
ipv6 ospf network	950
ipv6 ospf priority	951
ipv6 ospf retransmit-interval	952
ipv6 ospf transmit-delay	953
ipv6 router ospf	954
maximum-paths	954
nsf	955
nsf helper	956
nsf helper strict-lsa-checking	957
nsf restart-interval	958
passive-interface	959
passive-interface default	960
redistribute	960
router-id	961
show ipv6 ospf	962
show ipv6 ospf abr	966
show ipv6 ospf area	967
show ipv6 ospf asbr	968
show ipv6 ospf database	969

show ipv6 ospf database database-summary	972
show ipv6 ospf interface	973
show ipv6 ospf interface brief	974
show ipv6 ospf interface stats	975
show ipv6 ospf interface vlan	977
show ipv6 ospf neighbor	978
show ipv6 ospf range	980
show ipv6 ospf stub table	980
show ipv6 ospf virtual-link	981
show ipv6 ospf virtual-link brief	982
 46 PIM-DM Commands	 985
ip pimdm	986
show ip pimdm	986
show ip pimdm interface	987
show ip pimdm neighbor	988
 47 PIM-SM Commands	 989
ip pimsm	990
ip pimsm spt-threshold	990
ip pim-trapflags	991
show ip pimsm	992

show ip pimsm interface	992
show ip pimsm neighbor	993
show ip pimsm rphash.	994
 48 Router Discovery Protocol	
Commands	997
ip irdp	998
ip irdp address	998
ip irdp holdtime	999
ip irdp maxadvertinterval	1000
ip irdp minadvertinterval	1001
ip irdp multicast	1002
ip irdp preference	1003
show ip irdp	1004
 49 Routing Information Protocol	
Commands	1007
auto-summary	1008
default-information originate	1008
default-metric	1009
distance rip	1010
distribute-list out	1010
enable	1011

hostroutesaccept.	1012
ip rip	1013
ip rip authentication	1013
ip rip receive version	1014
ip rip send version	1015
redistribute.	1016
router rip	1017
show ip rip	1018
show ip rip interface.	1019
show ip rip interface brief.	1020
split-horizon	1021
 50 Tunnel Interface Commands	 1023
interface tunnel	1024
show interfaces tunnel	1024
tunnel destination	1025
tunnel mode ipv6ip.	1026
tunnel source.	1027
 51 Virtual LAN Routing Commands.	 1029
show ip vlan	1030

52 Virtual Router Redundancy Protocol Commands	1031
ip vrrp	1032
ip vrrp authentication	1033
ip vrrp ip	1034
ip vrrp mode	1035
ip vrrp preempt.	1035
ip vrrp priority	1036
ip vrrp timers advertise	1037
ip vrrp track interface	1038
ip vrrp track ip route.	1039
show ip vrrp	1040
show ip vrrp interface	1041
show ip vrrp interface brief	1042
show ip vrrp interface stats	1043
53 Autoconfig Commands	1045
boot host auto-save	1046
boot host dhcp	1046
boot host retry-count.	1047
show boot	1048

54 Captive Portal Commands	1049
authentication timeout.	1051
captive-portal	1051
enable	1052
http port.	1053
https port	1053
show captive-portal	1054
show captive-portal status	1055
block	1056
configuration.	1057
enable	1057
group	1058
interface	1059
locale.	1059
name	1060
protocol.	1061
redirect.	1061
redirect-url	1062
session-timeout	1062
verification	1063
captive-portal client deauthenticate	1064

show captive-portal client status	1064
show captive-portal configuration client status . . .	1066
show captive-portal interface client status	1067
show captive-portal interface configuration status	1069
clear captive-portal users	1070
no user	1070
show captive-portal user	1071
user group	1072
user name	1073
user password	1073
user session-timeout	1074
show captive-portal configuration	1075
show captive-portal configuration interface	1076
show captive-portal configuration locales	1077
show captive-portal configuration status	1078
show trapflags captive-portal	1079
user group	1080
user group moveusers	1081
user group name	1082

55 Clock Commands 1083

show clock	1083
show sntp configuration	1084
show sntp status	1085
sntp authenticate	1086
sntp authentication-key	1087
sntp broadcast client enable	1088
sntp client poll timer	1088
sntp server	1089
sntp trusted-key	1090
sntp unicast client enable	1091
clock timezone hours-offset	1092
no clock timezone	1092
clock summer-time recurring	1093
clock summer-time date	1094
no clock summer-time	1095
show clock	1096

56 Configuration and Image File Commands 1099

boot system	1100
clear config	1100

copy	1101
delete backup-config	1104
delete backup-image	1105
delete startup-config	1106
filedescr	1106
script apply	1107
script delete	1108
script list	1108
script validate	1110
show backup-config	1111
show bootvar	1112
show dir	1113
show running-config	1114
show startup-config	1115
update bootcode	1117
 57 Denial of Service Commands	 1119
dos-control firstfrag	1120
dos-control icmp	1120
dos-control l4port	1121
dos-control sipdip	1122
dos-control tcpflag	1123

dos-control tcpfrag	1123
ip icmp echo-reply	1124
ip icmp error-interval	1125
ip unreachablees	1126
ip redirects	1126
ipv6 icmp error-interval	1127
ipv6 unreachablees	1128
show dos-control	1128
 58 Line Commands	 1131
exec-timeout	1132
history	1132
history size	1133
line	1134
show line	1135
speed	1136
 59 Management ACL Commands	 1137
deny (management)	1138
management access-class	1139
management access-list	1140
permit (management)	1141

	show management access-class	1143
	show management access-list	1144
60 Password Management		
	Commands	1145
	passwords aging	1146
	passwords history	1146
	passwords lock-out	1147
	passwords min-length	1148
	show passwords configuration	1149
61 PHY Diagnostics Commands		1151
	show copper-ports cable-length	1152
	show copper-ports tdr	1153
	show fiber-ports optical-transceiver	1154
	test copper-port tdr	1155
62 Power Over Ethernet Commands		1157
	power inline	1158
	power inline legacy	1158
	power inline powered-device	1159
	power inline priority	1160

power inline traps	1161
power inline usage-threshold	1161
show poe-firmware-version	1162
show power inline	1163
show power inline ethernet	1164
 63 RMON Commands	 1167
rmon alarm	1168
rmon collection history	1169
rmon event	1171
show rmon alarm.	1172
show rmon alarm-table	1174
show rmon collection history	1175
show rmon events	1176
show rmon history	1177
show rmon log	1181
show rmon statistics.	1182
 64 Serviceability Tracing Packet Commands	 1187
debug arp.	1189
debug auto-voip	1189

debug clear	1190
debug console	1190
debug dot1x	1191
debug igmpsnooping.	1192
debug ip acl	1192
debug ip dvmrp.	1193
debug ip igmp	1194
debug ip mcache.	1195
debug ip pimdm	1195
debug ip pimsm	1196
debug ip vrrp	1197
debug ipv6 mcache	1198
debug ipv6 mld.	1198
debug ipv6 pimdm	1199
debug ipv6 pimsm	1200
debug isdp	1201
debug lacp	1201
debug mldsnooping	1202
debug ospf	1203
debug ospfv3	1203
debug ping	1204

debug rip	1205
debug sflow	1205
debug spanning-tree	1206
show debugging	1207
 65 sFlow Commands	1209
sflow destination	1210
sflow polling	1211
sflow polling (Interface Mode)	1212
sflow sampling	1213
sflow sampling (Interface Mode)	1214
show sflow agent	1215
show sflow destination	1216
show sflow polling	1217
show sflow sampling	1218
 66 SNMP Commands	1221
show snmp	1222
show snmp engineID	1223
show snmp filters	1224
show snmp groups	1225
show snmp users	1226

show snmp views	1227
show trapflags	1229
snmp-server community	1230
snmp-server community-group	1232
snmp-server contact	1233
snmp-server enable traps	1234
snmp-server enable traps authentication	1235
snmp-server engineID local	1236
snmp-server filter	1237
snmp-server group	1239
snmp-server host	1240
snmp-server location	1242
snmp-server user	1243
snmp-server view	1244
snmp-server v3-host	1246
 67 SSH Commands	 1249
crypto key generate dsa	1250
crypto key generate rsa	1250
crypto key pubkey-chain ssh	1251
ip ssh port	1252
ip ssh pubkey-auth	1253

ip ssh server	1254
key-string.	1254
show crypto key mypubkey	1256
show crypto key pubkey-chain ssh	1257
show ip ssh.	1259
user-key	1260
 68 Syslog Commands	 1261
clear logging	1262
clear logging file	1262
description	1263
level	1264
logging cli-command	1264
logging	1265
logging buffered	1266
logging console	1267
logging facility	1268
logging file	1268
logging on	1269
logging snmp	1270
logging web-session.	1271
port	1271

show logging	1272
show logging file	1274
show syslog-servers	1275
 69 System Management Commands	1277
asset-tag	1279
banner motd	1279
banner motd acknowledge	1280
clear checkpoint statistics	1281
cut-through mode	1282
hostname	1283
initiate failover	1283
member	1284
movemanagement	1285
no standby	1286
nsf	1288
ping	1288
reload	1290
set description	1291
show boot-version	1292
show checkpoint statistics	1292
show cut-through mode	1293

show memory cpu	1294
show nsf	1295
show process cpu	1296
show sessions	1299
show stack-port	1300
show stack-port counters	1301
show stack-port diag	1303
show stack-standby	1305
show supported switchtype	1306
show switch	1308
show system	1314
show system id	1316
show tech-support	1317
show users	1319
show version	1320
stack	1321
stack-port	1322
standby	1323
switch priority	1323
switch renumber	1324

telnet	1325
traceroute	1327
70 Telnet Server Commands	1331
ip telnet server disable	1332
ip telnet port	1332
show ip telnet	1333
71 User Interface Commands	1335
enable	1336
end	1336
exit	1337
quit	1338
72 Web Server Commands	1339
common-name	1340
country	1340
crypto certificate generate	1341
crypto certificate import	1342
crypto certificate request	1344
duration	1345
ip http port	1345

ip http server	1346
ip https certificate	1347
ip https port.	1347
ip https server	1348
key-generate	1349
location.	1350
organization-unit.	1350
show crypto certificate mycertificate.	1351
show ip http	1352
show ip https.	1353
state	1355

Command Groups

Introduction

The Command Line Interface (CLI) is a network management application operated through an ASCII terminal without the use of a Graphic User Interface (GUI) driven software application. By directly entering commands, the user has greater configuration flexibility. The CLI is a basic command-line interpreter similar to the UNIX C shell.

A switch can be configured and maintained by entering commands from the CLI, which is based solely on textual input and output with commands being entered by a terminal keyboard and the output displayed as text via a terminal monitor. The CLI can be accessed from a console terminal connected to an EIA/TIA-232 port or through a Telnet session.

This guide describes how the CLI is structured, describes the command syntax, and describes the command functionality.

This guide also provides information for configuring the PowerConnect switch, details the procedures, and provides configuration examples. Basic installation configuration is described in the *User's Guide* and must be completed before using this document.

Command Groups

The system commands can be broken down into three sets of functional groups, Layer 2, Layer 3, and Utility.

Table 1-1. System Command Groups

Command Group	Description
Layer 2 Commands	
AAA	Configures connection security including authorization and passwords.
ACL	Configures and displays ACL information.

Table 1-1. System Command Groups (continued)

Command Group	Description
Address Table	Configures bridging address tables.
CDP Interoperability	Configures Cisco Discovery Protocol (CDP).
DHCP I2 Relay	Enables the Layer 2 DHCP Relay agent for an interface.
DHCP Snooping	Configures DHCP snooping and whether an interface is trusted for filtering.
Dynamic ARP Inspection	Configures for rejection of invalid and malicious ARP packets.
Ethernet Configuration	Configures all port configuration options for example ports, storm control, port speed and auto-negotiation.
GVRP	Configures and displays GVRP configuration and information.
IGMP Snooping	Configures IGMP snooping and displays IGMP configuration and IGMP information.
IGMP Snooping Querier	Configures IGMP Snooping Querier and displays IGMP Snooping Querier information.
IP Addressing	Configures and manages IP addresses on the switch.
IPv6 ACL	Configures and displays ACL information for IPv6.
IPv6 MLD Snooping	Configures IPv6 MLD Snooping.
IPv6 MLD Snooping Querier	Configures IPv6 Snooping Querier and displays IPv6 Snooping Querier information.
iSCSI Optimization	Configures special treatment for traffic between iSCSI initiators and target systems and allows the switch to automatically discover Dell EqualLogic arrays via LLDP.
LACP	Configures and displays LACP information.
Link Dependency	Configures and displays link dependency information.
LLDP	Configures and displays LLDP information.
Port Channel	Configures and displays Port channel information.
Port Monitor	Monitors activity on specific target ports.
QoS	Configures and displays QoS information.
Radius	Configures and displays RADIUS information.

Table 1-1. System Command Groups *(continued)*

Command Group	Description
Spanning Tree	Configures and reports on Spanning Tree protocol.
Switchport Voice	Configures the Auto VoIP feature.
TACACS+	Configures and displays TACACS+ information.
VLAN	Configures VLANs and displays VLAN information.
Voice VLAN	Configures voice VLANs and displays voice VLAN information.
802.1x	Configures and displays commands related to 802.1x security protocol.
Layer 3 Commands	
ARP (IPv4)	Manages Address Resolution Protocol functions.
DHCP and BOOTP Relay (IPv4)	Manages DHCP/BOOTP operations on the system.
DHCPv6	Configures IPv6 DHCP functions.
DVMRP (Mcast)	Configures DVMRP operations.
IGMP (Mcast)	Configures IGMP operations.
IGMP Proxy (Mcast)	Manages IGMP Proxy on the system.
IP Helper	Configures relay of UDP packets.
IP Routing (IPv4)	Configures IP routing and addressing.
IPv6 Multicast	Manages IPv6 Multicasting on the system.
IPv6 Routing	Configures IPv6 routing and addressing.
Loopback Interface (IPv6)	Manages Loopback configurations.
Multicast (Mcast)	Manages Multicasting on the system.
OSPF (IPv4)_	Manages shortest path operations.
OSPFv3 (IPv6)	Manages IPv6 shortest path operations.
PIM-DM (Mcast)	Configures PIM-DM operations.
PIM-SM (Mcast)	Configures PIM-SM operations.

Table 1-1. System Command Groups (continued)

Command Group	Description
Router Discovery Protocol (IPv4)	Manages router discovery operations.
Routing Information Protocol (IPv4)	Configures RIP activities.
Tunnel Interface (IPv6)	Managing tunneling operations.
Virtual LAN Routing (IPv4)	Controls virtual LAN routing.
Virtual Router Redundancy (IPv4)	Manages router redundancy on the system.
Utility Commands	
Auto Config	Automatically configures switch when a configuration file is not found.
Captive Portal	Blocks clients from accessing network until user verification is established.
Clock	Configures the system clock.
Configuration and Image Files	Manages the switch configuration files.
Denial of Service	Provides several Denial of Service options.
Line	Configures the console, SSH, and remote Telnet connection.
Management ACL	Configures and displays management access-list information.
Password Management	Provides password management.
PHY Diagnostics	Diagnoses and displays the interface status.
Power Over Ethernet (PoE)	Configures PoE and displays PoE information.
RMON	Can be configured through the CLI and displays RMON information.
Serviceability Tracing	Controls display of debug output to serial port or telnet console.
sFlow	Configures sFlow monitoring.

Table 1-1. System Command Groups *(continued)*

Command Group	Description
SNMP	Configures SNMP communities, traps and displays SNMP information.
SSH	Configures SSH authentication.
Syslog	Manages and displays syslog messages.
System Management	Configures the switch clock, name and authorized users.
Telnet Server	Configures Telnet service on the switch and displays Telnet information.
User Interface	Describes user commands used for entering CLI commands.
Web Server	Configures web-based access to the switch.

Mode Types

The tables on the following pages use these abbreviations for Command Mode names.

- ARPA — ARP ACL Configuration
- CC — Crypto Configuration
- CP — Captive Portal Configuration
- CPI — Captive Portal Instance
- CMC — Class-Map Configuration
- GC — Global Configuration
- IC — Interface Configuration
- IP — IP Access List Configuration
- KC — Key Chain
- KE — Key
- L — Logging
- LC — Line Configuration
- MA — Management Access-level
- MC — MST Configuration
- ML — MAC-ACL Configuration
- PE — Privileged EXEC
- PM — Policy Map Configuration
- PCGC — Policy Map Global Configuration
- PCMC — Policy Class Map Configuration
- R — Radius
- RIP — Router RIP Configuration
- RC — Router Configuration
- ROSPF — Router Open Shortest Path First
- ROSV3 — Router Open Shortest Path First Version 3
- SG — Stack Global Configuration
- SP — SSH Public Key

- SK — SSH Public Key-chain
- TC — TACACS Configuration
- UE — User EXEC
- VLAN — VLAN Configuration
- v6ACL — IPv6 Access List Configuration
- v6CMC
- v6DP — IPv6 DHCP Pool Configuration

Layer 2 Commands

AAA

Command	Description	Mode*
aaa authentication dot1x	Specifies one or more authentication, authorization and accounting (AAA) methods for use on interfaces running IEEE 802.1X.	GC
aaa authentication enable	Defines authentication method lists for accessing higher privilege levels.	GC
aaa authentication login	Defines login authentication.	GC
aaa authorization network default radius	Enables the switch to accept VLAN assignment by the RADIUS server.	GC
enable authentication	Specifies the authentication method list when accessing a higher privilege level from a remote telnet or console.	LC
enable password	Sets a local password to control access to the normal level.	GC
ip http authentication	Specifies authentication methods for http.	GC
ip https authentication	Specifies authentication methods for https.	GC
login authentication	Specifies the login authentication method list for a remote telnet or console.	LC
password	Specifies a password on a line.	LC
password	Specifies a user password	UE

Command	Description	Mode*
show authentication methods	Shows information about authentication methods	PE
show user accounts	Displays information about the local user database	PE
show users login-history	Displays information about login histories of users	PE
username	Establishes a username-based authentication system.	GC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

ACL

Command	Description	Mode*
access-list	Creates an Access Control List (ACL) that is identified by the parameter <i>accesslistnumber</i> .	GC
deny permit	The deny command denies traffic if the conditions defined in the deny statement are matched. The permit command allows traffic if the conditions defined in the permit statement are matched.	ML
ip access-group	Attaches a specified access-control list to an interface.	GC or IC
ip access-group <name> out	Applies an IP based egress ACL on an Ethernet interface or a group of interfaces.	IC
mac access-group	Attaches a specific MAC Access Control List (ACL) to an interface in a given direction.	GC or IC
mac access-list extended	Creates the MAC Access Control List (ACL) identified by the <i>name</i> parameter.	GC
mac access-list extended rename	Renames the existing MAC Access Control List (ACL) name.	GC

Command	Description	Mode*
show ip access-lists	Displays an Access Control List (ACL) and all of the rules that are defined for the ACL.	PE
show mac access-list	Displays a MAC access list and all of the rules that are defined for the ACL.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Address Table

Command	Description	Mode*
bridge address	Adds a static MAC-layer station source address to the bridge table.	IC
bridge aging-time	Sets the address table aging time.	GC
bridge multicast address	Registers MAC-layer Multicast addresses to the bridge table, and adds static ports to the group.	IC
bridge multicast filtering	Enables filtering of Multicast addresses.	GC
bridge multicast forbidden address	Forbids adding a specific Multicast address to specific ports.	IC
bridge multicast forbidden forward-unregistered	Forbids a port to be a forwarding-unregistered-multicast-addresses port.	IC
bridge multicast forward-all	Enables forwarding of all Multicast packets on a port.	IC
bridge multicast forward-unregistered	Enables the forwarding of unregistered multicast addresses	IC
clear bridge	Removes any learned entries from the forwarding database.	PE
port security	Disables new address learning on an interface.	IC
port security max	Configures the maximum addresses that can be learned on the port while the port is in port security mode.	IC
show bridge address-table	Displays dynamically created entries in the bridge-forwarding database.	PE
show bridge address-table count	Displays the number of addresses present in the Forwarding Database.	PE

Command	Description	Mode*
show bridge address-table static	Displays statically created entries in the bridge-forwarding database.	PE
show bridge multicast address-table	Displays Multicast MAC address table information.	PE
show bridge multicast filtering	Displays the Multicast filtering configuration.	PE
show ports security	Displays the port-lock status.	PE
show ports security addresses	Displays current dynamic addresses in locked ports.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

CDP Interoperability

Command	Description	Mode*
clear isdp counters	Clears the ISDP counters.	PE
clear isdp table	Clears entries in the ISDP table.	PE
isdp advertise-v2	Enables the sending of ISDP version 2 packets from the device.	GC
isdp enable	Enables ISDP on the switch.	GC/IC
isdp holdtime	Configures the hold time for ISDP packets that the switch transmits.	GC
isdp timer	Sets period of time between sending new ISDP packets.	GC
show isdp	Displays global ISDP settings.	PE
show isdp interface	Displays ISDP settings for the specified interface.	PE
show isdp entry	Displays ISDP entries.	PE
show isdp neighbors	Displays the list of neighboring devices.	PE
show isdp traffic	Displays ISDP statistics.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

DHCP I2 Relay

Command	Description	Mode*
dhcp l2relay	Enables the Layer 2 DHCP Relay agent for an interface.	GC/IC
dhcp l2relay circuit-id	Enables user to set the DHCP Option 82 Circuit ID for a VLAN.	GC
dhcp l2relay remote-id	Enables user to set the DHCP Option 82 Remote ID for a VLAN.	GC
dhcp l2relay vlan	Enables the L2 DHCP Relay agent for a set of VLANs.	GC
dhcp l2relay trust	Configures an interface to trust a received DHCP Option 82.	IC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

DHCP Snooping

Command	Description	Mode*
clear ip dhcp snooping binding	Clears all DHCP Snooping entries.	PE
clear ip dhcp snooping statistics	clears all DHCP Snooping statistics.	PE
ip dhcp snooping	Enables DHCP snooping globally or on a specific VLAN.	GC/IC
ip dhcp snooping binding	Configures a static DHCP Snooping binding.	GC
ip dhcp snooping database	Configures the persistent location of the DHCP snooping database.	GC
ip dhcp snooping database write-delay	Configures the interval in seconds at which the DHCP Snooping database will be stored in persistent storage.	GC
ip dhcp snooping limit	Controls the maximum rate of DHCP messages.	IC
ip dhcp snooping log-invalid	Enables logging of DHCP messages filtered by the DHCP Snooping application.	IC

Command	Description	Mode*
ip dhcp snooping trust	Configure a port as trusted for DHCP snooping.	IC
ip dhcp snooping verify mac-address	Enables the verification of the source MAC address with the client MAC address in the received DHCP message.	GC
show ip dhcp snooping	Displays the DHCP snooping global and per port configuration.	PE
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.	PE
show ip dhcp snooping database	Displays the DHCP snooping configuration related to the database persistence.	PE
show ip dhcp snooping interfaces	Displays the DHCP Snooping status of the interfaces.	PE
show ip dhcp snooping statistics	Displays the DHCP snooping filtration statistics.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Dynamic ARP Inspection

Command	Description	Mode*
arp access-list	Creates an ARP ACL.	GC
clear counters ip arp inspection	Resets the statistics for Dynamic ARP Inspection on all VLANs.	PE
ip arp inspection filter	Configures the ARP ACL to be used for a single VLAN or a range of VLANs to filter invalid ARP packets.	GC
ip arp inspection limit	Configures the rate limit and burst interval values for an interface.	IC
ip arp inspection trust	Configures an interface as trusted for Dynamic ARP Inspection.	IC
ip arp inspection validate	Enables additional validation checks like source MAC address validation, destination MAC address validation or IP address validation on the received ARP packets.	GC

Command	Description	Mode*
ip arp inspection vlan	Enables Dynamic ARP Inspection on a single VLAN or a range of VLANs.	GC
permit ip host mac host	Configures a rule for a valid IP address and MAC address combination used in ARP packet validation.	ARPA
show arp access-list	Displays the configured ARP ACLs with the rules.	PE
show ip arp inspection ethernet	Displays the Dynamic ARP Inspection configuration on all the DAI enabled interfaces.	PE
show ip arp inspection statistics	Displays the statistics of the ARP packets processed by Dynamic ARP Inspection.	PE
show ip arp inspection vlan	Displays the Dynamic ARP Inspection configuration on all the VLANs in the given VLAN range.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Ethernet Configuration

Command	Description	Mode*
clear counters	Clears statistics on an interface.	PE
description	Adds a description to an interface.	IC
duplex	Configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation.	IC
flowcontrol	Configures the flow control on a given interface.	GC
interface ethernet	Enters the interface configuration mode to configure an Ethernet type interface.	GC
interface range ethernet	Enters the interface configuration mode to configure multiple Ethernet type interfaces.	GC
mtu	Enables jumbo frames on an interface by adjusting the maximum size of a packet or maximum transmission unit (MTU).	IC

Command	Description	Mode*
negotiation	Enables auto-negotiation operation for the speed and duplex parameters of a given interface.	IC
show interfaces advertise	Displays information about auto negotiation advertisement.	PE
show interfaces configuration	Displays the configuration for all configured interfaces.	UE
show interfaces counters	Displays traffic seen by the physical interface.	UE
show interfaces description	Displays the description for all configured interfaces.	UE
show interfaces detail	Displays the detail for all configured interfaces.	UE
show interfaces status	Displays the status for all configured interfaces.	UE
show statistics ethernet	Displays statistics for one port or for the entire switch.	PE
show storm-control	Displays the storm control configuration.	PE
shutdown	Disables interfaces.	IC
speed	Configures the speed of a given Ethernet interface when not using auto-negotiation.	IC
storm-control broadcast	Enables Broadcast storm control.	IC
storm-control multicast	Enables the switch to count Multicast packets together with Broadcast packets.	IC
storm-control unicast	Enables Unicast storm control.	IC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

GVRP

Command	Description	Mode*
clear gvrp statistics	Clears all the GVRP statistics information.	PE
garp timer	Adjusts the GARP application join, leave, and leaveall GARP timer values.	IC
gvrp enable (global)	Enables GVRP globally.	GC

Command	Description	Mode*
gvrp enable (interface)	Enables GVRP on an interface.	IC
gvrp registration-forbid	De-registers all VLANs, and prevents dynamic VLAN registration on the port.	IC
gvrp vlan-creation-forbid	Enables or disables dynamic VLAN creation.	IC
show gvrp configuration	Displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP	PE
show gvrp error-statistics	Displays GVRP error statistics.	UE
show gvrp statistics	Displays GVRP statistics.	UE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IGMP Snooping

Command	Description	Mode*
ip igmp snooping (Global)	In Global Config mode, Enables Internet Group Management Protocol (IGMP) snooping.	GC
ip igmp snooping (Interface)	Enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN.	IC
ip igmp snooping host-time-out	Configures the host-time-out.	IC
ip igmp snooping leave-time-out	Configures the leave-time-out.	IC
ip igmp snooping mrouter-time-out	Configures the mrouter-time-out.	IC
show ip igmp snooping groups	Displays Multicast groups learned by IGMP snooping.	UE
show ip igmp snooping interface	Displays IGMP snooping configuration.	PE
show ip igmp snooping mrouter	Displays information on dynamically learned Multicast router interfaces.	PE

Command	Description	Mode*
ip igmp snooping (VLAN)	In VLAN Config mode, enables IGMP snooping on a particular VLAN or on all interfaces participating in a VLAN.	VLAN
ip igmp snooping fast-leave	Enables or disables IGMP Snooping fast-leave mode on a selected VLAN.	VLAN
ip igmp snooping groupmembership-interval	Sets the IGMP Group Membership Interval time on a VLAN.	VLAN
ip igmp snooping maxresponse	Sets the IGMP Maximum Response time on a particular VLAN.	VLAN
ip igmp snooping mcertexpiretime	Sets the Multicast Router Present Expiration time.	VLAN
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IGMP Snooping Querier

Command	Description	Mode*
ip igmp snooping querier	Enables/disables IGMP Snooping Querier on the system (Global Configuration mode) or on a VLAN.	GC, VLAN
ip igmp snooping querier election participate	Enables the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN.	VLAN
ip igmp snooping querier query-interval	Sets the IGMP Querier Query Interval time.	GC
ip igmp snooping querier timer expiry	Sets the IGMP Querier timer expiration period.	GC
ip igmp snooping querier version	Sets the IGMP version of the query that the snooping switch is going to send periodically.	GC
show igmp snooping querier	Displays IGMP Snooping Querier information.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IP Addressing

Command	Description	Mode*
clear host	Deletes entries from the host name-to-address cache	PE
helper address	Enable forwarding User Datagram Protocol (UDP) Broadcast packets received on an interface.	IC
ip address	Sets a management IP address on the switch.	GC
ip address dhcp	Acquires an IP address on an interface from the DHCP server.	GC
ip address vlan	Sets the management VLAN.	GC
ip default-gateway	Defines a default gateway (router).	GC
ip domain-lookup	Enables IP DNS-based host name-to-address translation.	GC
ip domain-name	Defines a default domain name to complete unqualified host names.	GC
ip host	Configures static host name-to-address mapping in the host cache.	GC
ip name-server	Configures available name servers.	GC
ipv6 address	Set the IPv6 address of the management interface.	GC
ipv6 enable	Enable IPv6 on the management interface.	GC
ipv6 gateway	Configures an IPv6 gateway for the management interface.	GC
show arp switch	Displays the entries in the ARP table.	PE
show hosts	Displays the default domain name, a list of name server hosts, static and cached list of host names and addresses.	UE
show ip helper-address	Displays the ip helper addresses configuration.	PE
show ip interface management	Displays the management IP interface information.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IPv6 ACL

Command	Description	Mode*
{deny permit}	Creates a new rule for the current IPv6 access list.	v6ACL
ipv6 access-list	Creates an IPv6 Access Control List (ACL) consisting of classification fields defined for the IP header of an IPv6 frame.	GC
ipv6 access-list rename	Changes the name of an IPv6 ACL.	GC
ipv6 traffic-filter	Attaches a specific IPv6 ACL to an interface or associates it with a VLAN ID in a given direction.	GC IC
show ipv6 access-lists	Displays an IPv6 access list (and the rules defined for it).	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IPv6 MLD Snooping

Command	Description	Mode*
ipv6 mld snooping immediate-leave	Enables or disables MLD Snooping immediate-leave admin mode on a selected interface or VLAN.	IC VLAN
ipv6 mld snooping groupmembership-interval	Sets the MLD Group Membership Interval time on a VLAN or interface.	IC VLAN
ipv6 mld snooping maxresponse	Sets the MLD Maximum Response time for an interface or VLAN.	IC VLAN
ipv6 mld snooping mrcexpiretime	Sets the Multicast Router Present Expiration time.	IC
ipv6 mld snooping (Global)	Enables MLD Snooping on the system (Global Config Mode).	GC
ipv6 mld snooping (Interface)	Enables MLD Snooping on an interface.	IC
ipv6 mld snooping (VLAN)	Enables MLD Snooping on a particular VLAN and all interfaces participating in that VLAN.	VLAN

Command	Description	Mode*
show ipv6 mld snooping	Displays MLD Snooping information.	PE
show ipv6 mld snooping groups	Displays the MLD Snooping entries in the MFDB table.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IPv6 MLD Snooping Querier

Command	Description	Mode*
ipv6 mld snooping querier	Enables MLD Snooping Querier on the system or on a VLAN.	GC VLAN
ipv6 mld snooping querier address	Sets the global MLD Snooping Querier address on the system or on a VLAN.	GC VLAN
ipv6 mld snooping querier election participate	Enables the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN.	VLAN
ipv6 mld snooping querier query-interval	Sets the MLD Querier Query Interval time.	GC
ipv6 mld snooping querier timer expiry	Sets the MLD Querier timer expiration period.	GC
show ipv6 mld snooping querier	Displays MLD Snooping Querier information.	PE
show ipv6 mld snooping groups	Displays the MLD Snooping entries in the MFDB table.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

iSCSI Optimization

Command	Description	Mode*
iscsi enable	Globally enables iSCSI awareness.	GC
show iscsi	Displays the iSCSI settings.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

LACP

Command	Description	Mode*
lacp port-priority	Configures the priority value for physical ports.	IC
lacp system-priority	Configures the system LACP priority.	GC
lacp timeout	Assigns an administrative LACP timeout.	IC
show lacp ethernet	Displays LACP information for Ethernet ports.	PE
show lacp port-channel	Displays LACP information for a port-channel.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Link Dependency

Command	Description	Mode*
link-dependency group	Enters the link-dependency mode to configure a link-dependency group.	GC
no link-dependency group	Removes the configuration for a link-dependency group.	GC
add ethernet	Adds member Ethernet port(s) to the dependency list.	Link Dependency
no add ethernet	Removes member Ethernet port(s) from the dependency list.	Link Dependency
add port-channel	Adds member port-channels to the dependency list.	Link Dependency
no add port-channel	Removes member port-channels from the dependency list.	Link Dependency
depends-on ethernet	Adds the dependent Ethernet ports list.	Link Dependency
no depends-on ethernet	Removes the dependent Ethernet ports list.	Link Dependency
depends-on port-channel	Adds the dependent port-channels list.	Link Dependency

Command	Description	Mode*
no depends-on port-channel	Removes the dependent port-channels list.	Link Dependency
show link-dependency	Shows the link dependencies configured on a particular group.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

LLDP

Command	Description	Mode*
clear lldp remote data	Deletes all data from the remote data table.	PE
clear lldp statistics	Resets all LLDP statistics.	PE
lldp notification	Enables remote data change notifications.	IC
lldp notification-interval	Limits how frequently remote data change notifications are sent.	GC
lldp receive	Enables the LLDP receive capability.	IC
lldp timers	Sets the timing parameters for local data transmission on ports enabled for LLDP.	GC
lldp transmit	Enables the LLDP advertise capability.	IC
lldp transmit-mgmt	Specifies that transmission of the local system management address information in the LLDPDU is included.	IC
lldp transmit-tlv	Specifies which optional TLVs in the 802.1AB basic management set will be transmitted in the LLDPDU.	IC
show lldp	Displays the current LLDP configuration summary.	PE
show lldp connections	Displays the current LLDP remote data.	PE
show lldp interface	Displays the current LLDP interface state.	PE
show lldp local-device	Displays the LLDP local data	PE
show lldp remote-device	Displays the LLDP remote data	PE

Command	Description	Mode*
show lldp statistics	Displays the current LLDP traffic statistics.	PE
lldp med	Enables/disables LLDP-MED on an interface.	IC
lldp med transmit-tlv	Spwcifies which optional TLVs in the LLDP MED set are transmitted in the LLDPDUs.	IC
lldp med faststartrepeatcount	Sets the value of the fast start repeat count.	GC
lldp med confignotification	Enables sending the topology change notifications.	IC
show lldp med	Displays a summary of the current LLDP MED configuration.	PE
show lldp med interface	Displays a summary of the current LLDP MED configuration for a specific interface.	PE
show lldp med remote-device	Displays the current LLDP MED remote data.	PE
show lldp med local-device	Displays the advertised LLDP local data.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Port Channel

Command	Description	Mode*
channel-group	Associates a port with a port-channel.	IC
interface port-channel	Enters the interface configuration mode of a specific port-channel.	GC
interface range port-channel	Enters the interface configuration mode to configure multiple port-channels.	GC
hashing-mode	Sets the hashing algorithm on trunk ports.	IC (port-channel)
no hashing-mode	Sets the hashing algorithm on trunk ports to default (3).	IC (port-channel)

Command	Description	Mode*
show interfaces port-channel	Displays port-channel information.	PE
show statistics port-channel	Displays port-channel statistics.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Port Monitor

Command	Description	Mode*
monitor session	Configures a port monitoring session.	GC
show monitor session	Displays the port monitoring status.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

QoS

Command	Description	Mode*
assign-queue	Modifies the queue ID to which the associated traffic stream is assigned.	PCM C
class	Creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements.	PMC
class-map	Defines a new DiffServ class of type <i>match-all</i> , <i>match-any</i> , or <i>match-access-group</i> . For now, only <i>match-all</i> is available in the CLI.	GC
class-map rename	Changes the name of a DiffServ class.	GC
classofservice dot1p-mapping	Maps an 802.1p priority to an internal traffic class for a switch.	GC and IC
classofservice ip-dscp-mapping	Maps an IP DSCP value to an internal traffic class.	GC
classofservice trust	Sets the class of service trust mode of an interface.	GC and IC

Command	Description	Mode*
conform-color	Specifies for each outcome, the only possible actions are drop, setdscp-transmit, set-prec-transmit, or transmit	PCM C
cos-queue min-bandwidth	Specifies the minimum transmission bandwidth for each interface queue.	GC and IC
cos-queue strict	Activates the strict priority scheduler mode for each specified queue.	GC and IC
diffserv	Sets the DiffServ operational mode to active.	GC
drop	Use the drop policy-class-map configuration command to specify that all packets for the associated traffic stream are to be dropped at ingress.	PCM C
mark cos	Marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header.	PCM C
mark ip-dscp	Marks all packets for the associated traffic stream with the specified IP DSCP value.	PCM C
mark ip-precedence	Marks all packets for the associated traffic stream with the specified IP precedence value.	PCM C
match class-map	Adds add to the specified class definition the set of match conditions defined for another class.	CMC
match cos	Adds to the specified class definition a match condition for the Class of Service value.	CMC
match destination-address mac	Adds to the specified class definition a match condition based on the destination MAC address of a packet.	CMC
match dstip	Adds to the specified class definition a match condition based on the destination IP address of a packet.	CMC
match dstip6	adds to the specified class definition a match condition based on the destination IPv6 address of a packet.	v6CM C

Command	Description	Mode*
match dsl4port	Adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword, or a numeric notation.	CMC
match ethertype	Adds to the specified class definition a match condition based on the value of the ethertype.	CMC
match ip6flowlbl	Adds to the specified class definition a match condition based on the IPv6 flow label of a packet.	v6CM C
match ip dscp	Adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet.	CMC
match ip precedence	Adds to the specified class definition a match condition based on the value of the IP	CMC
match ip tos	Adds to the specified class definition a match condition based on the value of the IP TOS field in a packet.	CMC
match protocol	Adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.	CMC
match source-address mac	Adds to the specified class definition a match condition based on the source MAC address of the packet.	CMC
match srcip	Adds to the specified class definition a match condition based on the source IP address of a packet.	CMC
match srcip6	Adds to the specified class definition a match condition based on the source IPv6 address of a packet.	v6CM C
match srcl4port	Adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword, a numeric notation, or a numeric range notation.	CMC

Command	Description	Mode*
match vlan	Adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field.	CMC
mirror	Mirrors all the data that matches the class defined to the destination port specified	PCM C
police-simple	Establishes the traffic policing style for the specified class.	PCM C
policy-map	Establishes a new DiffServ policy	GC
redirect	Specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).	PCM C
service-policy	Attaches a policy to an interface in a particular direction.	GC and IC
show class-map	Displays all configuration information for the specified class.	PE
show classofservice dot1p-mapping	Displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface.	PE
show classofservice ip-dscp-mapping	Displays the current IP DSCP mapping to internal traffic classes for a specific interface.	PE
show classofservice trust	Displays the current trust mode setting for a specific interface.	PE
show diffserv	Displays the DiffServ General Status information.	PE
show diffserv service interface ethernet in	Displays policy service information for the specified interface and direction.	PE
show diffserv service interface port-channel in	Displays policy service information for the specified interface and direction.	PE
show diffserv service brief	Displays all interfaces in the system to which a DiffServ policy has been attached.	PE
show interfaces cos-queue	Displays the class-of-service queue configuration for the specified interface.	PE

Command	Description	Mode*
show policy-map	Displays all configuration information for the specified policy.	PE
show policy-map interface	Displays policy-oriented statistics information for the specified interface and direction	PE
show service-policy	Displays a summary of policy-oriented statistics information for all interfaces in the specified direction.	PE
traffic-shape	Specifies the maximum transmission bandwidth limit for the interface as a whole.	GC and IC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Radius

Command	Description	Mode*
aaa accounting network default start-stop group radius	Enables RADIUS accounting on the switch.	GC
auth-port	Sets the port number for authentication requests of the designated radius server.	R
deadtime	Improves Radius response times when a server is unavailable by causing the unavailable server to be skipped.	R
key	Sets the authentication and encryption key for all RADIUS communications between the switch and the RADIUS daemon.	R
msgauth	Enables the message authenticator attribute to be used for the RADIUS Authenticating server being configured.	R
name	Assigns a name to a RADIUS server.	R
primary	Specifies that a configured server should be the primary server in the group of authentication servers which have the same server name.	R
priority	Specifies the order in which the servers are to be used, with 0 being the highest priority.	R

Command	Description	Mode*
radius-server deadtime	Improves RADIUS response times when servers are unavailable. Causes the unavailable servers to be skipped.	GC
radius-server host	Specifies a RADIUS server host.	GC
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the switch and the RADIUS daemon.	GC
radius-server retransmit	Specifies the number of times the software searches the list of RADIUS server hosts.	GC
radius-server source-ip	Specifies the source IP address used for communication with RADIUS servers.	GC
radius-server timeout	Sets the interval for which a switch waits for a server host to reply	GC
retransmit	Specifies the number of times the software searches the list of RADIUS server hosts before stopping the search.	R
show radius-servers	Displays the RADIUS server settings.	PE
show radius-servers statistics	Shows the statistics for an authentication or accounting server.	PE
source-ip	Specifies the source IP address to be used for communication with RADIUS servers.	R
timeout	Sets the timeout value in seconds for the designated radius server.	R
usage	Specifies the usage type of the server.	R
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Spanning Tree

Command	Description	Mode*
clear spanning-tree detected-protocols	Restarts the protocol migration process on all interfaces or on the specified interface.	PE
exit (mst)	Exits the MST configuration mode and applies configuration changes.	MC

Command	Description	Mode*
instance (mst)	Maps VLANs to an MST instance.	MC
name (mst)	Defines the MST configuration name.	MC
revision (mst)	Defines the configuration revision number.	MC
show spanning-tree	Displays spanning tree configuration.	PE
show spanning-tree summary	Displays spanning tree settings and parameters for the switch.	PE
spanning tree	Enables spanning-tree functionality.	GC
spanning-tree auto-portfast	Sets the port to auto portfast mode.	IC
spanning-tree bpdu	Defines the bridge protocol data unit (BPDU) handling when spanning tree is disabled on an interface.	GC
spanning-tree bpdu flooding	Allows flooding of BPDUs received on nonspanning-tree ports to all other non-spanning-tree ports.	GC
spanning-tree bpdu-protection	Enables BPDU protection on a switch.	GC
spanning-tree cost	Configures the spanning tree path cost for a port.	IC
spanning-tree disable	Disables spanning tree on a specific port.	IC
spanning-tree forward-time	Configures the spanning tree bridge forward time.	GC
spanning-tree guard	Selects whether loop guard or root guard is enabled on an interface.	IC
spanning-tree link-type	Overrides the default link-type setting.	IC
spanning-tree loopguard	Enables loop guard on all ports.	GC
spanning-tree max-age	Configures the spanning tree bridge maximum age.	GC
spanning-tree max-hops	Sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree.	GC
spanning-tree mode	Configures the spanning tree protocol.	GC

Command	Description	Mode*
spanning-tree mst configuration	Enables configuring an MST region by entering the multiple spanning-tree (MST) mode.	GC
spanning-tree mst 0 external-cost	Sets the external cost for the common spanning tree.	IC
spanning-tree mst cost	Configures the path cost for multiple spanning tree (MST) calculations.	IC
spanning-tree mst port-priority	Configures port priority.	IC
spanning-tree mst priority	Configures the switch priority for the specified spanning tree instance.	GC
spanning-tree pathcost method	Configures the spanning tree default pathcost method	GC
spanning-tree portfast	Enables PortFast mode.	IC
spanning-tree portfast bpdupfilter default	Discards BPDU received on spanningtree ports in portfast mode.	GC
spanning-tree portfast default	Enables Portfast mode on all ports.	GC
spanning-tree port-priority	Configures port priority.	IC
spanning-tree priority	Configures the spanning tree priority.	GC
spanning-tree tcnguard	Prevents a port from propagating topology change notifications.	IC
spanning-tree transmit hold-count	Set the maximum number of BPDUs that a bridge is allowed to send within a hello time window (2 seconds).	GC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Switchport Voice

Command	Description	Mode*
switchport voice detect auto	Enables the VoIP Profile on all the interfaces of the switch.	GC/IC
show switchport voice	Displays the status of auto-voip on an interface or all interfaces.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

TACACS+

Command	Description	Mode*
key	Specifies the authentication and encryption key for all TACACS communications between the device and the TACACS server.	TC
port	Specifies a server port number.	TC
priority	Specifies the order in which servers are used.	TC
show tacacs	Displays TACACS+ server settings and statistics.	PE
tacacs-server host	Specifies a TACACS+ server host.	GC
tacacs-server key	Sets the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon.	GC
tacacs-server timeout	Sets the interval for which the switch waits for a server host to reply.	GC
timeout	Specifies the timeout value in seconds.	TC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

VLAN

Command	Description	Mode*
dvlan-tunnel ethertype	Configures the EtherType for the interface.	GC
interface vlan	Enters the interface configuration (VLAN) mode.	GC

Command	Description	Mode*
interface range vlan	Enters the interface configuration mode to configure multiple VLANs.	GC
mode dvlan-tunnel	Enables Double VLAN tunneling on the specified interface	IC
name	Configures a name to a VLAN.	IC
protocol group	Attaches a <i>vlanid</i> to the protocol-based VLAN identified by <i>groupid</i> .	VLAN
protocol vlan group	Adds the physical unit/port interface to the protocol-based VLAN identified by <i>groupid</i> .	IC
protocol vlan group all	Adds all physical unit/port interfaces to the protocol-based VLAN identified by <i>groupid</i> .	GC
show dvlan-tunnel	Displays all interfaces enabled for Double VLAN Tunneling.	PE
show dvlan-tunnel interface	Displays detailed information about Double VLAN Tunneling for the specified interface.	PE
show interfaces switchport	Displays switchport configuration.	PE
show port protocol	Displays the Protocol-Based VLAN information for either the entire system or for the indicated group	PE
show switchport protected	Displays protected group/port information.	PE
show vlan	Displays VLAN information.	PE
show vlan association mac	Displays the VLAN associated with a specific configured MAC address.	PE
show vlan association subnet	Displays the VLAN associated with a specific configured IP subnet.	PE
switchport access vlan	Configures the VLAN ID when the interface is in access mode.	IC
switchport forbidden vlan	Forbids adding specific VLANs to a port.	IC
switchport general acceptable-frame-type tagged-only	Discards untagged frames at ingress.	IC

Command	Description	Mode*
switchport general allowed vlan	Adds or removes VLANs from a port in General mode.	IC
switchport general ingress-filtering disable	Disables port ingress filtering.	IC
switchport general pvid	Configures the PVID when the interface is in general mode.	IC
switchport mode	Configures the VLAN membership mode of a port.	IC
switchport protected	Sets the port to Protected mode.	IC
switchport protected name	Configures a name for a protected group	GC
switchport trunk allowed vlan	Adds or removes VLANs from a port in general mode.	IC
vlan	Creates a VLAN.	VLAN
vlan association mac	Associates a MAC address to a VLAN.	VLAN
vlan association subnet	Associates an IP subnet to a VLAN	VLAN
vlan database	Enters the VLAN database configuration mode.	GC
vlan makestatic	Changes a dynamically created VLAN to a static VLAN.	VLAN
vlan protocol group	Adds protocol-based VLAN groups to the system.	GC
vlan protocol group add protocol	Adds a protocol to the protocol-based VLAN identified by <i>groupid</i> .	GC
vlan protocol group name	Adds a group name to the protocol-based VLAN identified by <i>groupid</i> .	GC
vlan protocol group remove	Removes the protocol-base VLAN group identified by <i>groupid</i> .	GC
vlan routing	Enable routing on a VLAN.	PE
* NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Voice VLAN

Command	Description	Mode*
voice vlan	Enables the voice VLAN capability on the switch.	GG
voice vlan	Enables the voice VLAN capability on the interface	IC
voice vlan data priority	Trusts or not trusts the data traffic arriving on the voice VLAN port.	IC
show voice vlan	Displays various properties of the voice VLAN.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

802.1x

Command	Description	Mode*
dot1x mac-auth-bypass	Enables MAB on an interface.	IC
dot1x max-req	Sets the maximum number of times the switch sends an EAP-request frame to the client before restarting the authentication process.	IC
dot1x max-users	Sets the maximum number of clients supported on the port when MAC-based 802.1X authentication is enabled on the port.	IC
dot1x port-control	Enables manual control of the authorization state of the port.	IC
dot1x re-authenticate	Manually initiates a re-authentication of all 802.1x-enabled ports or a specified 802.1X enabled port.	PE
dot1x re-authentication	Enables periodic re-authentication of the client.	IC
dot1x system-auth-control	Enables 802.1X globally.	GC
dot1x timeout quiet-period	Sets the number of seconds the switch remains in the quiet state following a failed authentication attempt	IC
dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.	IC

Command	Description	Mode*
dot1x timeout server-timeout	Sets the number of seconds the switch waits for a response from the authentication server before resending the request.	IC
dot1x timeout supp-timeout	Sets the number of seconds the switch waits for a response to an EAP-request frame from the client before retransmitting the request.	IC
dot1x timeout tx-period	Sets the number of seconds the switch waits for a response to an EAP-request/identify frame from the client before resending the request.	IC
show dot1x	Displays 802.1X status for the switch or the specified interface.	PE
show dot1x clients	Displays detailed information about the users who have successfully authenticated on the system or on a specified port.	PE
show dot1x ethernet	Shows the status of MAC Authentication Bypass.	PE
show dot1x statistics	Displays 802.1X statistics for the specified interface.	PE
show dot1x users	Displays active 802.1X authenticated users for the switch.	PE
dot1x guest-vlan	Sets the guest VLAN on a port.	IC
dot1x unauth-vlan	Specifies the unauthenticated VLAN on a port.	IC
dot1x guest-vlan	Defines a guest VLAN.	IC
show dot1x advanced	Displays 802.1X advanced features for the switch or specified interface.	PE
radius-server attribute 4	Sets the network access server (NAS) IP address for the RADIUS server.	GC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Layer 3 Commands

ARP (IPv4)

Command	Description	Mode*
arp	Creates an Address Resolution Protocol (ARP) entry.	GC
arp cachesize	Configures the maximum number of entries in the ARP cache.	GC
arp dynamicrenew	Enables the ARP component to automatically renew dynamic ARP entries when they age out.	GC
arp purge	Causes the specified IP address to be removed from the ARP cache.	PE
arp resptime	Configures the ARP request response timeout.	GC
arp retries	Configures the ARP count of maximum request for retries.	GC
arp timeout	Configures the ARP entry age-out time.	GC
clear arp-cache	Removes all ARP entries of type dynamic from the ARP cache.	PE
clear arp-cache management	Removes all entries from the ARP cache learned from the management port.	PE
ip proxy-arp	Enables proxy ARP on a router interface.	IC
show arp	Displays the Address Resolution Protocol (ARP) cache.	PE
show arp brief	Displays the brief Address Resolution Protocol (ARP) table information.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

DHCP and BOOTP Relay (IPv4)

Command	Description	Mode*
bootpdhcprelay cidridoptmode	Enables the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the system.	GC
bootpdhcprelay maxhopcount	Configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system.	GC
bootpdhcprelay minwaittime	Configures the minimum wait time in seconds for BootP/DHCP Relay on the system.	GC
show bootpdhcprelay	Shows the the BootP/DHCP Relay information.	GC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

DHCPv6

Command	Description	Mode*
clear ipv6 dhcp	Clears DHCPv6 statistics for all interfaces or for a specific interface.	PE
dns-server	Sets the ipv6 DNS server address which is provided to a DHCPv6 client by the DHCPv6 server.	v6DP
domain-name	Sets the DNS domain name which is provided to a DHCPv6 client by the DHCPv6 server.	v6DP
ipv6 dhcp pool	Enters IPv6 DHCP Pool Configuration mode.	GC
ipv6 dhcp relay	Configures an interface for DHCPv6 relay functionality.	IC
ipv6 dhcp relay-agent-info-opt	Configures a number to represent the DHCPv6 Relay Agent Information Option.	GC
ipv6 dhcp relay-agent-info-remote-id-subopt	Configures a number to represent the DHCPv6 the "remote-id" sub-option.	GC
ipv6 dhcp server	Configures DHCPv6 server functionality on an interface.	IC
prefix-delegation	Defines Multiple IPv6 prefixes within a pool for distributing to specific DHCPv6 Prefix delegation clients.	v6DP

Command	Description	Mode*
service dhcpv6	Enables DHCPv6 configuration on the router.	GC
show ipv6 dhcp	Displays the DHCPv6 server name and status.	PE
show ipv6 dhcp binding	Displays the configured DHCP pool.	PE
show ipv6 dhcp interface	Displays DHCPv6 information for all relevant interfaces or a specified interface.	UE
show ipv6 dhcp pool	Displays the configured DHCP pool.	PE
show ipv6 dhcp statistics	Displays the DHCPv6 server name and status.	UE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

DVMRP

Command	Description	Mode*
ip dvmrp	Sets the administrative mode of DVMRP in the router to active.	GC IC
ip dvmrp metric	Configures the metric for an interface.	IC
ip dvmrp trapflags	Enables the DVMRP trap mode.	GC
show ip dvmrp	Displays the system-wide information for DVMRP.	PE
show ip dvmrp interface	Displays the interface information for DVMRP on the specified interface.	PE
show ip dvmrp neighbor	Displays the neighbor information for DVMRP.	PE
show ip dvmrp nexthop	Displays the next hop information on outgoing interfaces for routing multicast datagrams.	PE
show ip dvmrp prune	Displays the table that lists the router's upstream prune information.	PE
show ip dvmrp route	Displays the multicast routing information for DVMRP.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IGMP

Command	Description	Mode*
ip igmp	Sets the administrative mode of IGMP in the system to active.	GC
ip igmp last-member-query-count	Sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface.	IC
ip igmp last-member-query-interval	Configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages.	IC
ip igmp query-interval	Configures the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface.	IC
ip igmp query-max-response-time	Configures the maximum response time interval for the specified interface.	IC
ip igmp robustness	Configures the robustness that allows tuning of the interface.	IC
ip igmp startup-query-count	Sets the number of queries sent out on startup—at intervals equal to the startup query interval for the interface.	IC
ip igmp startup-query-interval	Sets the interval between general queries sent at startup on the interface.	IC
ip igmp version	Configures the version of IGMP for an interface.	IC
show ip igmp	Displays system-wide IGMP information.	PE
show ip igmp groups	Displays the registered multicast groups on the interface.	PE
show ip igmp interface	Displays the IGMP information for the specified interface.	PE

Command	Description	Mode*
show ip igmp interface membership	Displays the list of interfaces that have registered in the multicast group.	PE
show ip igmp interface stats	Displays the IGMP statistical information for the interface.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IGMP Proxy

Command	Description	Mode*
ip igmp-proxy	Enables the IGMP Proxy on the router.	IC
ip igmp-proxy reset-status	Resets the host interface status parameters of the IGMP Proxy router.	IC
ip igmp-proxy unsolicited-report-interval	Sets the unsolicited report interval for the IGMP Proxy router.	IC
show ip igmp-proxy	Displays a summary of the host interface status parameters.	PE
show ip igmp-proxy interface	Displays a detailed list of the host interface status parameters.	PE
show ip igmp-proxy groups	Displays a table of information about multicast groups that IGMP Proxy reported.	PE
show ip igmp-proxy groups detail	Displays complete information about multicast groups that IGMP Proxy has reported.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IP Helper

Command	Description	Mode*
clear ip helper statistics	Resets (to 0) the statistics displayed in show ip helper statistics.	PE
ip helper-address (global configuration)	Configures the relay of certain UDP broadcast packets received on any interface.	GC
ip helper-address (interface configuration)	Configures the relay of certain UDP broadcast packets received on a specific interface.	IC

Command	Description	Mode*
ip helper enable	Enables relay of UDP packets.	GC
show ip helper-address	Displays the IP helper address configuration.	PE
show ip helper statistics	Displays the number of DHCP and other UDP packets processed and relayed by the UDP relay agent.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IP Routing

Command	Description	Mode*
encapsulation	Configures the link layer encapsulation type for the packet.	IC
ip address	Configures an IP address on an interface.	IC
ip mtu	Sets the IP Maximum Transmission Unit (MTU) on a routing interface.	IC
ip netdirbcast	Enables the forwarding of network-directed broadcasts.	IC
ip route	Configures a static route. Use the no form of the command to delete the static route.	GC
ip route default	Configures the default route. Use the no form of the command to delete the default route.	GC
ip route distance	Sets the default distance (preference) for static routes.	GC
ip routing	Globally enables IPv4 routing on the router.	GC
routing	Enables IPv4 and IPv6 routing for an interface.	IC
show ip brief	Displays all the summary information of the IP.	PE
show ip interface	Displays all pertinent information about the IP interface.	PE
show ip protocols	Displays the parameters and current state of the active routing protocols.	PE
show ip route	Displays the routing table.	PE

Command	Description	Mode*
show ip route preferences	Displays detailed information about the route preferences.	PE
show ip route summary	Shows the number of all routes, including best and non-best routes.	PE
show ip stats	Displays IP statistical information	UE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IPv6 Multicast

Command	Description	Mode*
ipv6 pimsm (Global config)	Administratively enables PIMSM for IPv6 multicast routing.	GC
ipv6 pimsm (VLAN Interface config)	Administratively enables PIM-SM multicast routing mode on a particular IPv6 router interface.	IC
ipv6 pimsm bsr-border	Prevents bootstrap router (BSR) messages from being sent or received through an interface.	IC
ipv6 pimsm bsr-candidate	Configures the router to announce its candidacy as a bootstrap router (BSR).	GC
ipv6 pimsm dr-priority	Sets the priority value for which a router is elected as the designated router (DR).	IC
ipv6 pimsm hello-interval	Configures the PIM-SM Hello Interval for the specified interface.	IC
ipv6 pimsm join-prune-interval	Configures the interface join/prune interval for the PIM-SM router	IC
ipv6 pimsm register-threshold	Configure the Register Threshold rate for the RP router to switch to the shortest path.	GC
ipv6 pimsm rp-address	Statically configures the RP address for one or more multicast groups.	GC
ipv6 pimsm rp-candidate	Configures the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).	GC

Command	Description	Mode*
ipv6 pimsm spt-threshold	Configures the Data Threshold rate for the lasthop router to switch to the shortest path.	GC
ipv6 pimsm ssm	Defines the Source Specific Multicast (SSM) range of multicast addresses.	GC
show ipv6 pimsm	Displays global status of IPv6 PIMSM and its IPv6 routing interfaces.	PE
show ipv6 pimsm bsr	Displays the bootstrap router (BSR) information.	PE
show ipv6 pimsm interface	Displays interface config parameters.	PE
show ipv6 pimsm neighbor	Displays IPv6 PIMSM neighbors learned on the routing interfaces.	PE
show ipv6 pimsm rphash	Displays which rendezvous point (RP) is being selected for a specified group.	PE
show ipv6 pimsm rp mapping	Displays all group-to-RP mappings of which the router is aware (either configured or learned from the BSR).	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

IPv6 Routing

Command	Description	Mode*
clear ipv6 neighbors	Clears all entries in the IPv6 neighbor table or an entry on a specific interface.	PE
clear ipv6 statistics	Clears IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces.	PE
ipv6 address	Configures an IPv6 address on an interface (including tunnel and loopback interfaces).	IC
ipv6 enable	Enables IPv6 routing on an interface (including tunnel and loopback interfaces) that has not been configured with an explicit IPv6 address.	IC
ipv6 forwarding	Enables IPv6 forwarding on a router.	GC

Command	Description	Mode*
ipv6 host	Defines static host name-to- ipv6 address mapping in the host cache.	GC
ipv6 mld last-member-query-count	Sets the number of listener-specific queries sent before the router assumes that there are no local members on the interface.	IC (VLAN)
ipv6 mld last-member-query-interval	Sets the last member query interval for the MLD interface, which is the value of the maximum response time parameter in the group-specific queries sent out of this interface.	IC (VLAN)
ipv6 mld-proxy	Enables MLD Proxy on the router.	IC
ipv6 mld-proxy reset-status	Resets the host interface status parameters of the MLD Proxy router.	IC
ipv6 mld-proxy unsolicit-rprt-interval	Sets the unsolicited report interval for the MLD Proxy router.	IC
ipv6 mld query-interval	Sets the MLD router's query interval for the interface.	IC
ipv6 mld query-max-response-time	Sets MLD querier's maximum response time for the interface.	IC
ipv6 mld router	Enables MLD in the router in global configuration mode and for a specific interface in interface configuration mode.	GC IC
ipv6 mtu	Sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface.	IC
ipv6 nd dad attempts	Sets the number of duplicate address detection probes transmitted while doing neighbor discovery.	IC
ipv6 nt managed-config-flag	Sets the “managed address configuration” flag in router advertisements.	IC
ipv6 nd ns-interval	Sets the interval between router advertisements for advertised neighbor solicitations.	IC
ipv6 nd other-config-flag	Sets the “other stateful configuration” flag in router advertisements sent from the interface.	IC
ipv6 nd prefix	Sets the IPv6 prefixes to include in the router advertisement.	IC

Command	Description	Mode*
ipv6 nd ra-interval	Sets the transmission interval between router advertisements.	IC
ipv6 nd ra-lifetime	Sets the value that is placed in the Router Lifetime field of the router advertisements sent from the interface.	IC
ipv6 nd reachable-time	Sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation.	IC
ipv6 nd suppress-ra	Suppresses router advertisement transmission on an interface.	IC
ipv6 pimdm	Enables PIM-DM Multicast Routing Mode across the router in global configuration mode or on a specific routing interface in interface mode.	GC IC
ipv6 pimdm query-interval	Configures the PIM-DM Hello Interval for the specified router interface.	IC
ipv6 route	Configures an IPv6 static route	GC
ipv6 route distance	Sets the default distance (preference) for static routes.	GC
ipv6 unicast-routing	Enables forwarding of IPv6 unicast datagrams.	GC
ping ipv6	Determines whether another computer is on the network.	PE
ping ipv6 interface	Determines whether another computer is on the network using Interface keyword.	PE
show ipv6 brief	Displays the IPv6 status of forwarding mode and IPv6 unicast routing mode.	PE
show ipv6 interface	Shows the usability status of IPv6 interfaces.	PE
show ipv6 mld groups	Displays information about multicast groups that MLD reported.	PE
show ipv6 mld interface	Displays MLD related information for an interface.	PE
show ipv6 mld-proxy	Displays a summary of the host interface status parameters.	PE

Command	Description	Mode*
show ipv6 mld-proxy groups	Displays information about multicast groups that the MLD Proxy reported.	PE
show ipv6 mld-proxy groups detail	Displays information about multicast groups that MLD Proxy reported.	PE
show ipv6 mld-proxy interface	Displays a detailed list of the host interface status parameters.	PE
show ipv6 mld traffic	Displays MLD statistical information for the router.	PE
show ipv6 neighbors	Displays information about IPv6 neighbors.	PE
show ipv6 pimdm	Displays PIM-DM Global Configuration parameters and PIM DM interface status.	PE
show ipv6 pimdm neighbor	Displays PIM-DM Neighbor information including Neighbor Address, Uptime and Expiry time for all interfaces or for the specified interface.	PE
show ipv6 pimdm interface	Displays PIM-DM Configuration information for all interfaces or for the specified interface.	PE
show ipv6 neighbors	Displays information about the IPv6 neighbors.	PE
show ipv6 route	Displays the IPv6 routing table.	PE
show ipv6 route preference	Shows the preference value associated with the type of route.	PE
show ipv6 route summary	Displays a summary of the routing table.	PE
show ipv6 traffic	Shows traffic and statistics for IPv6 and ICMPv6.	UE
show ipv6 vlan	Displays IPv6 VLAN routing interface addresses.	PE
traceroute ipv6	Discovers the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Loopback Interface

Command	Description	Mode*
interface loopback	Enters the Interface Loopback configuration mode.	GC
show interface loopback	Displays information about configured loopback interfaces.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Multicast

Command	Description	Mode*
ip mcast boundary	Adds an administrative scope multicast boundary.	IC
ip mroute	Creates a static multicast route for a source range.	GC
ip multicast	Sets the administrative mode of the IP multicast forwarder in the router to active.	GC
ip multicast ttl-threshold	Applies a <i>ttlvalue</i> to a routing interface.	IC
ip pimsm	Administratively enables PIM-SM multicast routing mode on a particular router interface.	IC
ip pimsm bsr-border	Prevents bootstrap router (BSR) messages from being sent or received through an interface.	IC
ip pimsm bsr-candidate	Configures the router to announce its candidacy as a bootstrap router (BSR).	GC
ip pimsm dr-priority	Sets the priority value for which a router is elected as the designated router (DR).	IC
ip pimsm hello-interval	Configures the PIM-SM Hello Interval for the specified interface.	IC
ip pimsm join-prune-interval	Configures the interface join/prune interval for the PIM-SM router.	IC
ip pimsm register-threshold	Configures the Register Threshold rate for the RP router to switch to the shortest path.	GC

Command	Description	Mode*
ip pimsm rp-address	Statically configures the RP address for one or more multicast groups.	GC
ip pimsm rp-candidate	Configures the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).	IC
ip pimsm spt-threshold	Configures the Data Threshold rate for the lasthop router to switch to the shortest path.	GC
ip pimsm ssm	Defines the Source Specific Multicast (SSM) range of IP multicast addresses.	GC
show bridge multicast address-table count	Displays statistical information about the entries in the multicast address table.	PE
show ip mcast	Displays the system-wide multicast information.	PE
show ip mcast boundary	Displays the system-wide multicast information.	PE
show ip mcast interface	Displays the multicast information for the specified interface.	PE
show ip mcast mroute	Displays a summary or all the details of the multicast table.	PE
show ip mcast mroute group	Displays the multicast configuration settings of entries in the multicast mroute table.	PE
show ip mcast mroute source	Displays the multicast configuration settings of entries in the multicast mroute table.	PE
show ip mcast mroute static	Displays all the static routes configured in the static mcast table.	PE
show ip pimsm bsr	Displays the bootstrap router (BSR) information.	PE
show ip pimsm interface	Displays interface config parameters. If no interface is specified, all interfaces are displayed.	PE
show ip pimsm rp-hash	Displays which rendezvous point (RP) is being selected for a specified group.	PE

Command	Description	Mode*
show ip pimsm rp mapping	Displays all group-to-RP mappings of which the router is aware (either configured or learned from the bootstrap router).	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

OSPF

Command	Description	Mode*
area default-cost	Configures the monetary default cost for the stub area.	ROSPF
area nssa	Configures the specified area ID to function as an NSSA.	ROSPF
area nssa default-info-originate	Configures the metric value and type for the default route advertised into the NSSA.	ROSPF
area nssa no-redistribute	Configures the NSSA Area Border router (ABR) so that learned external routes are not redistributed to the NSSA.	ROSPF
area nssa no-summary	Configures the NSSA so that summary LSAs are not advertised into the NSSA.	ROSPF
area nssa translator-role	Configures the translator role of the NSSA.	ROSPF
area nssa translator-stab-intv	Configures the translator stability interval of the NSSA.	ROSPF
area range	Creates a specified area range for a specified NSSA.	ROSPF
area stub	Creates a stub area for the specified area ID.	ROSPF
area stub no-summary	Prevents Summary LSAs from being advertised into the NSSA.	ROSPF
area virtual-link	Creates the OSPF virtual interface for the specified area-id and neighbor router.	ROSPF
area virtual-link authentication	Configures the authentication type and key for the OSPF virtual interface identified by the area ID and neighbor ID.	ROSPF

Command	Description	Mode*
area virtual-link dead-interval	Configures the dead interval for the OSPF virtual interface on the virtual interface identified by area-id and neighbor router.	ROSPF
area virtual-link hello-interval	Configures the hello interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.	ROSPF
area virtual-link retransmit-interval	Configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.	ROSPF
area virtual-link transmit-delay	Configures the transmit delay for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID.	ROSPF
auto-cost	Allows user to change the reference bandwidth used in computing link cost.	ROSPF
bandwidth	Allows user to change the bandwidth used in computing link cost.	IC
capability opaque	Enables Opaque Capability on the router.	RC
clear ip ospf	Resets specific OSPF states.	PE
default-information originate	Controls the advertisement of default routes.	ROSPF
default-metric	Sets a default for the metric of distributed routes.	ROSPF
distance ospf	Sets the route preference value of OSPF in the router.	ROSPF
distribute-list out	Specifies the access list to filter routes received from the source protocol.	ROSPF
enable	Resets the default administrative mode of OSPF in the router (active).	ROSPF
exit-overflow-interval	Configures the exit overflow interval for OSPF.	ROSPF
external-lsdb-limit	Configures the external LSDB limit for OSPF.	ROSPF
ip ospf area	Enables OSPFv2 and sets the area ID of an interface.	IC
ip ospf authentication	Sets the OSPF Authentication Type and Key for the specified interface.	IC

Command	Description	Mode*
ip ospf cost	Configures the cost on an OSPF interface.	IC
ip ospf dead-interval	Sets the OSPF dead interval for the specified interface.	IC
ip ospf hello-interval	Sets the OSPF hello interval for the specified interface.	IC
ip ospf mtu-ignore	Disables OSPF maximum transmission unit (MTU) mismatch detection.	IC
ip ospf network	Configure OSPF to treat an interface as a point-to-point rather than broadcast interface.	IC
ip ospf priority	Sets the OSPF priority for the specified router interface.	IC
ip ospf retransmit-interval	Sets the OSPF retransmit Interval for the specified interface.	IC
ip ospf transmit-delay	Sets the OSPF Transit Delay for the specified interface.	IC
maximum-paths	Sets the number of paths that OSPF can report for a given destination.	ROSPF
nsf	Enables OSPF graceful restart.	ROSPF
nsf helper	Allow OSPF to act as a helpful neighbor for a restarting router.	ROSPF
nsf helper strict-lsa-checking	Set an OSPF helpful neighbor exit helper mode whenever a topology change occurs.	ROSPF
nsf restart-interval	Configures the length of the grace period on the restarting router.	ROSPF
network area	Enables OSPFv2 on an interface and sets its area ID if the IP address of an interface is covered by this network command.	ROSPF
passive-interface	Sets the interface or tunnel as passive.	IC
passive-interface default	Enables the global passive mode by default for all interfaces.	ROSPF

Command	Description	Mode*
passive-interface (router mode)	Sets the interface or tunnel as passive.	ROSPF
redistribute	Configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.	ROSPF
router-id	Sets a 4-digit dotted-decimal number uniquely identifying the router OSPF ID.	ROSPF
router ospf	Enters Router OSPF mode.	GC
show ip ospf	Displays information relevant to the OSPF router.	PE
show ip ospf abr	Displays the internal OSPF routing table entries to Area Border Routers (ABR).	PE
show ip ospf area	Displays information about the identified OSPF area.	PE
show ip ospf asbr	Displays the internal OSPF routing table entries to Autonomous System Boundary Routes (ASBR).	PE
show ip ospf database	Displays information about the link state database when OSPF is enabled.	PE
show ip ospf database database-summary	Displays the number of each type of LSA in the database for each area and for the router.	PE
show ip ospf interface	Displays the information for the IFO object or virtual interface tables.	PE
show ip ospf interface brief	Displays brief information for the IFO object or virtual interface tables.	PE
show ip ospf interface stats	Displays the statistics for a specific interface.	PE
show ip ospf neighbor	Displays information about OSPF neighbors.	PE
show ip ospf range	Displays information about the area ranges for the specified area-id.	PE
show ip ospf statistics	Displays information about recent Shortest Path First (SPF) calculations.	PE
show ip ospf stub table	Displays the OSPF stub table.	PE

Command	Description	Mode*
show ip ospf virtual-link	Displays the OSPF Virtual Interface information for a specific area and neighbor.	PE
show ip ospf virtual-link brief	Displays the OSPF Virtual Interface information for all areas in the system.	PE
timers spf	Configures the SPF delay and hold time.	ROSPF
trapflags	Enables OSPF traps.	ROSPF
1583compatibility	Enables OSPF 1583 compatibility.	ROSPF
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

OSPFv3

Command	Description	Mode*
area default-cost	Configures the monetary default cost for the stub area.	ROSV3
area nssa	Configures the specified areaid to function as an NSSA.	ROSV3
area nssa default-info-originate	Configures the metric value and type for the default route advertised into the NSSA.	ROSV3
area nssa no-redistribute	Configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.	ROSV3
area nssa no-summary	Configures the NSSA so that summary LSAs are not advertised into the NSSA.	ROSV3
area nssa translator-role	Configures the translator role of the NSSA.	ROSV3
area nssa translator-stab-intv	Configures the translator stability interval of the NSSA.	ROSV3
area range	Creates an area range for a specified NSSA.	ROSV3
area stub	Creates a stub area for the specified area ID.	ROSV3
area stub no-summary	Disables the import of Summary LSAs for the stub area identified by <i>areaid</i> .	ROSV3

Command	Description	Mode*
area virtual-link	Creates the OSPF virtual interface for the specified <i>areaid</i> and <i>neighbor</i> .	ROSV3
area virtual-link dead-interval	Configures the dead interval for the OSPF virtual interface on the virtual interface identified by <i>areaid</i> and <i>neighbor</i> .	ROSV3
area virtual-link hello-interval	Configures the hello interval for the OSPF virtual interface on the virtual interface identified by <i>areaid</i> and <i>neighbor</i> .	ROSV3
area virtual-link retransmit-interval	Configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by <i>areaid</i> and <i>neighbor</i> .	ROSV3
area virtual-link transmit-delay	Configures the transmit delay for the OSPF virtual interface on the virtual interface identified by <i>areaid</i> and <i>neighbor</i> .	ROSV3
default-information originate	Controls the advertisement of default routes.	ROSV3
default-metric	Sets a default for the metric of distributed routes.	ROSV3
distance ospf	Sets the route preference value of OSPF in the router.	ROSV3
enable	Resets the default administrative mode of OSPF in the router (active).	ROSV3
exit-overflow-interval	Configures the exit overflow interval for OSPF.	ROSV3
external-lsdb-limit	Configures the external LSDB limit for OSPF.	ROSV3
ipv6 ospf	Enables OSPF on a router interface or loopback interface.	IC
ipv6 ospf areaid	Sets the OSPF area to which the specified router interface belongs.	IC
ipv6 ospf cost	Configures the cost on an OSPF interface.	IC
ipv6 ospf dead-interval	Sets the OSPF dead interval for the specified interface.	IC
ipv6 ospf hello-interval	Sets the OSPF hello interval for the specified interface.	IC

Command	Description	Mode*
ipv6 ospf mtu-ignore	Disables OSPF maximum transmission unit (MTU) mismatch detection.	IC
ipv6 ospf network	Changes the default OSPF network type for the interface.	IC
ipv6 ospf priority	Sets the OSPF priority for the specified router interface.	IC
ipv6 ospf retransmit-interval	Sets the OSPF retransmit interval for the specified interface.	IC
ipv6 ospf transmit-delay	Sets the OSPF Transmit Delay for the specified interface.	IC
ipv6 router ospf	Enters Router OSPFv3 Configuration mode.	GC
maximum-paths	Sets the number of paths that OSPF can report for a given destination.	ROSV3
passive-interface	Sets the interface or tunnel as passive.	IC
passive-interface default	Enables the global passive mode by default for all interfaces.	ROSV3
redistribute	Configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.	ROSV3
router-id	Sets a 4-digit dotted-decimal number uniquely identifying the Router OSPF ID.	ROSV3
show ipv6 ospf	Displays information relevant to the OSPF router.	PE
show ipv6 ospf abr	Displays the internal OSPFv3 routes to reach Area Border Routers (ABR).	PE
show ipv6 ospf area	Displays information about the area.	PE
show ipv6 ospf asbr	Displays the internal OSPFv3 routes to reach Autonomous System Boundary Routes (ASBR).	PE
show ipv6 ospf database	Displays information about the link state database when OSPFv3 is enabled.	PE
show ipv6 ospf database database-summary	Displays the number of each type of LSA in the database and the total number of LSAs in the database.	PE

Command	Description	Mode*
show ipv6 ospf interface	Displays the information for the IFO object or virtual interface tables.	PE
show ipv6 ospf interface brief	Displays brief information for the IFO object or virtual interface tables.	PE
show ipv6 ospf interface stats	Displays the statistics for a specific interface.	UE
show ipv6 ospf interface vlan	Displays OSPFv3 configuration and status information for a specific vlan	PE
show ipv6 ospf neighbor	Displays information about OSPF neighbors.	PE
show ipv6 ospf range	Displays information about the area ranges for the specified area identifier.	PE
show ipv6 ospf stub table	Displays the OSPF stub table.	PE
show ipv6 ospf virtual-link	Displays the OSPF Virtual Interface information for a specific area and neighbor.	PE
show ipv6 ospf virtual-link brief	Displays the OSPFV3 Virtual Interface information for all areas in the system.	PE
trapflags	Enables OSPF traps	ROSV3
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

PIM-DM

Command	Description	Mode*
ip pimdm	Enables the administrative mode of PIM-DM in the router.	GC
ip pimdm mode	Sets administrative mode of PIM-DM on an interface to enabled.	IC
ip pimdm query-interval	Configures the transmission frequency of hello messages between PIM enabled neighbors.	IC
show ip pimdm	Displays system-wide information for PIM-DM.	PE
show ip pimdm interface	Displays interface information for PIM-DM on the specified interface.	PE

Command	Description	Mode*
show ip pimdm interface stats	Displays the statistical information for PIM-DM on the specified interface.	UE
show ip pimdm neighbor	Displays the neighbor information for PIM-DM on the specified interface.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

PIM-SM

Command	Description	Mode*
ip pimsm	Sets administrative mode of PIM-SM multicast routing across the router to enabled.	GC
ip pimsm cbsrhasmasklength	Configures the CBSR hash mask length to be advertised in bootstrap messages for a particular PIM-SM interface.	IC
ip pimsm cbsrpreference	Configures the CBSR preference for a particular PIM-SM interface.	IC
ip pimsm crppreference	Configures the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface.	IC
ip pimsm message-interval	Configures the global join/prune interval for PIM-SM router.	GC
ip pimsm mode	Sets to enabled the administrative mode of PIM-SM multicast routing on a routing interface.	IC
ip pimsm query-interval	Configures the transmission frequency of hello messages in seconds between PIM enabled neighbors.	IC
ip pimsm register-rate-limit	Sets the Register Threshold rate for the RP (Rendezvous Point) router to switch to the shortest path.	GC
ip pimsm spt-threshold	Configures the threshold rate for the RP router to switch to the shortest path.	GC
ip pimsm staticrp	Creates RP IP address for the PIM-SM router.	GC
ip pim-trapflags	Enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode (DM).	GC

Command	Description	Mode*
show ip pimsm	Displays the system-wide information for PIM-SM.	PE
show ip pimsm interface	Displays interface information for PIM-SM on the specified interface.	PE
show ip pimsm neighbor	Displays neighbor information for PIM-SM on the specified interface.	PE
show ip pimsm rphash	Displays the RP router being selected from the set of active RP routers.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Router Discovery Protocol

Command	Description	Mode*
ip irdp	Enables Router Discovery on an interface.	IC
ip irdp address	Configures the address that the interface uses to send the router discovery advertisements.	IC
ip irdp holdtime	Configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface.	IC
ip irdp maxadvertinterval	Configures the maximum time, in seconds, allowed between sending router advertisements from the interface.	IC
ip irdp minadvertinterval	Configures the minimum time, in seconds, allowed between sending router advertisements from the interface.	IC
ip irdp preference	Configures the preference of the address as a default router address relative to other router addresses on the same subnet.	IC
show ip irdp	Displays the router discovery information for all interfaces, or for a specified interface.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Routing Information Protocol

Command	Description	Mode*
auto-summary	Enables the RIP auto-summarization mode.	RIP
default-information originate	Controls the advertisement of default routes.	RIP
default-metric	Sets a default for the metric of distributed routes.	RIP
distance rip	Sets the route preference value of RIP in the router.	RIP
distribute-list out	Specifies the access list to filter routes received from the source protocol.	RIP
enable	Resets the default administrative mode of RIP in the router (active).	RIP
hostroutesaccept	Enables the RIP hostroutesaccept mode.	RIP
ip rip	Enables RIP on a router interface.	IC
ip rip authentication	Sets the RIP Version 2 Authentication Type and Key for the specified interface.	IC
ip rip receive version	Configures the interface to allow RIP control packets of the specified version(s) to be received.	IC
ip rip send version	Configures the interface to allow RIP control packets of the specified version to be sent.	IC
redistribute	Configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.	PIP
router rip	Enters Router RIP mode.	CC
show ip rip	Displays information relevant to the RIP router.	PE
show ip rip interface	Displays information related to a particular RIP interface.	PE

Command	Description	Mode*
show ip rip interface brief	Displays general information for each RIP interface.	PE
split-horizon	Sets the RIP split horizon mode.	RIP
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Tunnel Interface

Command	Description	Mode*
interface tunnel	Enables the interface configuration mode for a tunnel.	GC
show interface tunnel	Displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.	PE
tunnel destination	Specifies the destination transport address of the tunnel.	IC
tunnel mode ipv6ip	Specifies the mode of the tunnel.	IC
tunnel source	Specifies the source transport address of the tunnel, either explicitly or by reference to an interface.	IC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Virtual LAN Routing

Command	Description	Mode*
show ip vlan	Displays the VLAN routing information for all VLANs with routing enabled.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Virtual Router Redundancy

Command	Description	Mode*
ip vrrp	Enables the administrative mode of VRRP for the router.	GC

Command	Description	Mode*
ip vrrp authentication	Sets the authorization details value for the virtual router configured on a specified interface.	IC
ip vrrp ip	Sets the virtual router IP address value for an interface.	IC
ip vrrp mode	Enables the virtual router configured on an interface. Enabling the status field starts a virtual router.	IC
ip vrrp preempt	Sets the preemption mode value for the virtual router configured on a specified interface.	IC
ip vrrp priority	Sets the priority value for the virtual router configured on a specified interface.	IC
ip vrrp timers advertise	Sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.	IC
ip vrrp track interface	Alters the priority of the VRRP router based on the availability of its interfaces.	IC
ip vrrp track ip route	Tracks route reachability.	IC
show ip vrrp	Displays whether VRRP functionality is enabled or disabled on the switch.	PE
show ip vrrp interface	Displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface.	PE
show ip vrrp interface brief	Displays information about each virtual router configured on the switch.	PE
show ip vrrp interface stats	Displays the statistical information about each virtual router configured on the switch.	PE
vrrp track interface	Alters the priority of the VRRP router based on the availability of its interfaces.	IC
vrrp track ip route	Tracks route reachability.	IC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Utility Commands

Auto Config

Command	Description	Mode*
boot host auto-save	Enables/disables automatically saving the downloaded configuration on the switch.	GC
boot host dhcp	Enables/disables Auto Config on the switch.	GC
boot host retry-count	Set the number of attempts to download a configuration.	GC
show boot	Displays the current status of the Auto Config process.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Captive Portal

Command	Description	Mode*
authentication timeout	Configures the authentication timeout.	CP
captive-portal	Enables the captive portal configuration mode.	GC
http port	Configures an additional HTTP port for captive portal to monitor.	CP
https port	Configures an additional HTTPS port for captive portal to monitor.	CP
show captive-portal	Displays the status of captive portal.	PE
show captive-portal status	Reports the status of all captive portal instances in the system.	PE
block	Blocks all traffic for a captive portal configuration.	CPI
configuration	Enables the captive portal instance mode.	CP
enable	Globally enables captive portal.	CPI
group	Configures the group number for a captive portal configuration.	CPI

Command	Description	Mode*
interface	Associates an interface with a captive portal configuration.	CPI
locale	Associates an interface with a captive portal configuration.	CPI
name	Configures the name for a captive portal configuration.	CPI
protocol	Configures the protocol mode for a captive portal configuration.	CPI
redirect	Enables the redirect mode for a captive portal configuration.	CPI
redirect-url	Configures the redirect URL for a captive portal configuration,	CPI
session-timeout	Configures the session timeout for a captive portal configuration.	CPI
verification	Configures the verification mode for a captive portal configuration.	CPI
captive-portal client deauthenticate	Deauthenticates a specific captive portal client.	PE
show captive-portal client status	Displays client connection details or a connection summary for connected captive portal users.	PE
show captive-portal configuration client status	Displays the clients authenticated to all captive portal configurations or a to specific configuration.	PE
show captive-portal interface client status	Displays information about clients authenticated on all interfaces or a specific interface.	PE
show captive-portal interface configuration status	Displays the clients authenticated to all captive portal configurations or a to specific configuration.	PE
clear captive-portal users	Deletes all captive portal user entries.	PE
no user	Deletes a user from the local user database.	CP

Command	Description	Mode*
show captive-portal user	Displays all configured users or a specific user in the captive portal local user database.	PE
user idle-timeout	Sets the session idle timeout value for a captive portal user.	CP
user name	Modifies the user name for a local captive portal user.	CP
user password	Creates a local user or changes the password for an existing user.	CP
user session-timeout	Sets the session timeout value for a captive portal user.	CP
show captive-portal configuration	Displays the operational status of each captive portal configuration.	PE
show captive-portal configuration interface	Displays information about all interfaces assigned to a captive portal configuration or about a specific interface assigned to a captive portal configuration.	PE
show captive-portal configuration locales	Displays locales associated with a specific captive portal configuration.	PE
show captive-portal configuration status	Displays information about all configured captive portal configurations or a specific captive portal configuration.	PE
show captive-portal trapflags	Displays which captive portal traps are enabled.	PE
user group	Creates a user group.	CP
user group moveusers	Moves a group's users to a different group.	CP
user group name	Configures a group name.	CP
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Clock

Command	Description	Mode*
show clock	Displays the time and date of the system clock.	PE
show sntp configuration	Displays the SNTP configuration.	PE
show sntp status	Displays the SNTP status.	PE
sntp authenticate	Set to require authentication for received NTP traffic from servers.	GC
sntp authentication-key	Defines an authentication key for SNTP.	GC
sntp broadcast client enable	Enables SNTP Broadcast clients.	GC
sntp client enable	Enables SNTP Broadcast and Anycast clients on an interface.	IC
sntp client poll timer	Defines polling time for the SNTP client.	GC
sntp server	Configures the SNTP server to use SNTP to request and accept NTP traffic from it.	GC
sntp trusted-key	Authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize.	GC
sntp unicast client enable	Enables clients to use Simple Network Time Protocol (SNTP) predefined Unicast clients.	GC
clock timezone hours-offset	Sets the offset to Coordinated Universal Time.	GC
no clock timezone	Resets the time zone settings.	GC
clock summer-time recurring	Sets the summertime offset to UTC recursively every year.	GC
clock summer-time date	Sets the summertime offset to UTC.	GC
no clock summer-time	Resets the recurring summertime configuration.	GC
show clock	Displays the time and date from the system clock.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Configuration and Image Files

Command	Description	Mode*
boot system	Specifies the system image that the switch loads at startup.	PE
clear config	Restores switch to default configuration	PE
copy	Copies files from a source to a destination.	PE
delete backup-image	Deletes a file from a flash memory.	PE
delete backup-config	Deletes the backup configuration file	PE
delete startup-config	Deletes the startup configuration file.	PE
filedescr	Adds a description to a file.	PE
script apply	Applies commands in the script to the switch.	PE
script delete	Deletes a specific script.	PE
script list	Lists all scripts present in the switch.	PE
script show	Displays the contents of a script file.	PE
script validate	Validates a script file.	PE
show backup-config	Displays contents of a backup configuration file	PE
show bootvar	Displays the active system image file that the switch loads at startup.	UE
show dir	Lists all the files available on the flash file system.	PE
show running-config	Displays the contents of the currently running configuration file.	PE
show startup-config	Displays the startup configuration file contents.	PE
update bootcode	Updates the bootcode on one or more switches.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Denial of Service

Command	Description	Mode*
dos-control firstfrag	Enables Minimum TCP Header Size Denial of Service protection.	GC
dos-control icmp	Enables Maximum ICMP Packet Size Denial of Service protections.	GC
dos-control l4port	Enables L4 Port Denial of Service protection.	GC
dos-control sipdip	Enables Source IP Address = Destination IP Address (SIP=DIP) Denial of Service protection.	GC
dos-control tcpflag	Enables TCP Flag Denial of Service protections.	GC
dos-control tcpfrag	Enables TCP Fragment Denial of Service protection.	GC
ip icmp echo-reply	Enables or disables the generation of ICMP Echo Reply messages.	GC
ip icmp error-interval	Limits the rate at which IPv4 ICMP error messages are sent.	GC
ip icmp unreachable	Enables the generation of ICMP Destination Unreachable messages.	IC
ip icmp redirects	Enables the generation of ICMP Redirect messages.	IC
ipv6 icmp error-interval	Limits the rate at which ICMPv6 error messages are sent.	GC
ipv6 unreachable	Enables the generation of ICMPv6 Destination Unreachable messages.	IC
show dos-control	Displays Denial of Service configuration information.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Line

Command	Description	Mode*
exec-timeout	Configures the interval that the system waits for user input.	LC
history	Enables the command history function.	LC
history size	Changes the command history buffer size for a particular line.	LC
line	Identifies a specific line for configuration and enters the line configuration command mode.	GC
show line	Displays line parameters.	UE
speed	Sets the line baud rate.	LC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Management ACL

Command	Description	Mode*
deny (management)	Defines a deny rule.	MA
management access-class	Defines which management access-list is used.	GC
management access-list	Defines a management access-list, and enters the access-list for configuration.	GC
permit (management)	Defines a permit rule.	MA
show management access-class	Displays the active management access-list.	PE
show management access-list	Displays management access-lists.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Password Management

Command	Description	Mode*
passwords aging	Implements aging on the passwords such that users are required to change passwords when they expire.	GC
passwords history	Enables the administrator to set the number of previous passwords that are stored to ensure that users do not reuse their passwords too frequently.	GC
passwords lock-out	Enables the administrator to strengthen the security of the switch by enabling the user lockout feature. When a lockout count is configured, a user who is logging in must enter the correct password within that count.	GC
passwords min-length	Enables the administrator to enforce a minimum length required for a password.	GC
show passwords configuration	Displays the configuration parameters for password configuration.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

PHY Diagnostics

Command	Description	Mode*
show copper-ports cable-length	Displays the estimated copper cable length attached to a port.	PE
show copper-ports tdr	Displays the last TDR (Time Domain Reflectometry) tests on specified ports.	PE
show fiber-ports optical-transceiver	Displays the optical transceiver diagnostics.	PE
test copper-port tdr	Diagnoses with TDR (Time Domain Reflectometry) technology the quality and characteristics of a copper cable attached to a port.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Power Over Ethernet (PoE)

Command	Description	Mode*
power inline	Enables/disables the ability of the port to deliver power.	IC (Ethernet)
power inline legacy	Enables/disables the ability of the switch to support legacy Ethernet powered devices.	GC
power inline powered-device	Adds a comment or description of the powered device type.	IC (Ethernet)
power inline priority	Configures the port priority level for the delivery of power to an attached device.	IC (Ethernet)
power inline traps	Enables/disables inline power traps.	GC
power inline usage-threshold	Configures the system power usage threshold level at which a trap is generated.	GC
show poe-firmware-version	Displays the version of the PoE controller firmware present on the switch file system.	PE
show power inline	Displays the total available power, the total power consumed in the system, and the globally set usage threshold.	PE
show power inline ethernet	Displays the inline power summary for the interface.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

RMON

Command	Description	Mode*
rmon alarm	Configures alarm conditions.	GC
rmon collection history	Enables a Remote Monitoring (RMON) MIB history statistics group on an interface.	IC
rmon event	Configures an RMON event.	GC
show rmon alarm	Displays alarm configurations.	UE

Command	Description	Mode*
show rmon alarm-table	Displays the alarms summary table.	UE
show rmon collection history	Displays the requested group of statistics.	UE
show rmon events	Displays the RMON event table.	UE
show rmon history	Displays RMON Ethernet Statistics history.	UE
show rmon log	Displays the RMON logging table.	UE
show rmon statistics	Displays RMON Ethernet Statistics.	UE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Serviceability Tracing

Command	Description	Mode*
debug arp	Enables tracing of ARP packets.	PE
debug auto-voip	Enables Auto VOIP debug messages.	PE
debug clear	Disables all debug traces.	PE
debug console	Enables the display of debug trace output on the login session in which it is executed.	PE
debug dot1x	Enables dot1x packet tracing.	PE
debug igmpsnooping	Enables tracing of IGMP Snooping packets transmitted and/or received by the switch.	PE
debug ip acl	Enables debug of IP Protocol packets matching the ACL criteria.	PE
debug ip dvmrp	Traces DVMRP packet reception and transmission.	PE
debug ip igmp	Traces IGMP packet reception and transmission.	PE
debug ip mcache	Traces MDATA packet reception and transmission.	PE
debug ip pimdm	Traces PIMDM packet reception and transmission.	PE

Command	Description	Mode*
debug ip pimsm	Traces PIMSM packet reception and transmission.	PE
debug ip vrrp	Enables VRRP debug protocol messages.	PE
debug ipv6 mcache	Traces MDATAv6 packet reception and transmission.	PE
debug ipv6 mld	Traces MLD packet reception and transmission.	PE
debug ipv6 pimdm	Traces PIMDMv6 packet reception and transmission.	PE
debug ipv6 pimsm	Traces PIMSMv6 packet reception and transmission.	PE
debug isdp	Traces ISDP packet reception and transmission.	PE
debug lacp	Traces of LACP packets received and transmitted by the switch.	PE
debug mldsnoping	Traces MLD snooping packet reception and transmission.	PE
debug ospf	Enables tracing of OSPF packets received and transmitted by the switch.	PE
debug ospfv3	Enables tracing of OSPFv3 packets received and transmitted by the switch.	PE
debug ping	Enables tracing of ICMP echo requests and responses.	PE
debug rip	Enables tracing of RIP requests and responses.	PE
debug sflow	Enables sFlow debug packet trace.	PE
debug spanning-tree	Traces spanning tree BPDU packet reception and transmission.	PE
show debugging	Displays packet tracing configurations.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

sFlow

Command	Description	Mode*
sflow destination	Configures sFlow collector parameters (owner string, receiver timeout, ip address, and port).	GC
sflow polling	Enables a new sflow poller instance for the data source if rcvr_idx is valid.	GC
sflow polling (Interface Mode)	Enable a new sflow poller instance for this data source if rcvr_idx is valid.	IC
sflow sampling	Enables a new sflow sampler instance for this data source if rcvr_idx is valid.	GC
sflow sampling (Interface Mode)	Enables a new sflow sampler instance for this data source if rcvr_idx is valid.	IC
show sflow agent	Displays the sflow agent information.	PE
show sflow destination	Displays all the configuration information related to the sFlow receivers.	PE
show sflow polling	Displays the sFlow polling instances created on the switch.	PE
show sflow sampling	Displays the sFlow sampling instances created on the switch.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

SNMP

Command	Description	Mode*
show snmp	Displays the SNMP status.	PE
show snmp engineID	Displays the SNMP engine ID.	PE
show snmp filters	Displays the configuration of filters.	PE
show snmp groups	Displays the configuration of groups.	PE
show snmp users	Displays the configuration of users.	PE
show snmp views	Displays the configuration of views.	PE
show trapflags	Shows the status of the configurable SNMP traps.	PE

Command	Description	Mode*
snmp-server community	Sets up the community access string to permit access to SNMP protocol.	GC
snmp-server community-group	Maps SNMP v1 and v2 security models to the group name.	GC
snmp-server contact	Sets up a system contact (sysContact) string.	GC
snmp-server enable traps	Enables SNMP traps globally or enables specific SNMP traps.	GC
snmp-server engineID local	Specifies the Simple Network Management Protocol (SNMP) engine ID on the local switch.	GC
snmp-server filter	Creates or updates an SNMP server filter entry.	GC
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.	GC
snmp-server host	Specifies the recipient of SNMP notifications.	GC
snmp-server location	Sets the system location string.	GC
snmp-server enable traps authentication	Enables the switch to send SNMP traps when authentication failed.	GC
snmp-server v3-host	Specifies the recipient of SNMPv3 notifications.	GC
snmp-server user	Configures a new SNMP Version 3 user.	GC
snmp-server view	Creates or updates a Simple Network Management Protocol (SNMP) server view entry.	GC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

SSH

Command	Description	Mode*
crypto key generate dsa	Generates DSA key pairs for the switch.	GC
crypto key generate rsa	Generates RSA key pairs for the switch.	GC
crypto key pubkey-chain ssh	Enters SSH Public Key-chain configuration mode.	GC
ip ssh port	Specifies the port to be used by the SSH server.	GC

Command	Description	Mode*
ip ssh pubkey-auth	Enables public key authentication for incoming SSH sessions.	GC
ip ssh server	Enables the switch to be configured from a SSH server connection.	GC
key-string	Manually specifies a SSH public key.	SK
show crypto key mypubkey	Displays its own SSH public keys stored on the switch.	PE
show crypto key pubkey-chain ssh	Displays SSH public keys stored on the switch.	PE
show ip ssh	Displays the SSH server configuration.	PE
user-key	Specifies which SSH public key is manually configured and enters the SSH public key-string configuration command.	SP
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Syslog

Command	Description	Mode*
clear logging	Clears messages from the internal logging buffer.	PE
clear logging file	Clears messages from the logging file.	PE
description	Describes the syslog server.	L
level	Specifies the importance level of syslog messages.	L
login cli-command	Enable CLI command logging	GC
logging	Logs messages to a syslog server	GC
logging buffered	Limits syslog messages displayed from an internal buffer based on severity.	GC
logging console	Limits messages logged to the console based on severity.	GC
logging facility	Sets the facility of the logging messages.	GC

Command	Description	Mode*
logging file	Limits syslog messages sent to the logging file based on severity.	GC
logging on	Controls error messages logging.	GC
port	Specifies the port number of syslog messages.	L
show logging	Displays the state of logging and the syslog messages stored in the internal buffer.	PE
show logging file	Displays the state of logging and the syslog messages stored in the logging file.	PE
show syslog-servers	Displays the syslog servers settings.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

System Management

Command	Description	Mode*
asset-tag	Specifies the switch asset-tag.	GC
banner motd	Specifies message-of-the-day banner.	GC
banner motd acknowledge	Acknowledges message-of-the-day banner.	GC
show checkpoint statistics	Shows the checkpointing status.	PE
clear checkpoint statistics	Clears the statistics for the checkpointing process.	GC
cut-through mode	Enables the cut-through mode on the switch.	GC
hostname	Specifies or modifies the switch host name.	GC
initiate failover	Forces failover of management unit.	GC
member	Configures the switch.	SG
movemanagement	Moves the Management Switch functionality from one switch to another.	SG
nsf	Specifies non-stop forwarding.	GC
nsf restart-interval	Specifies the length of the grace period on the restarting router.	GC

Command	Description	Mode*
no cut-through mode	Disables the cut-through mode on the switch.	GC
no standby	Removes standby configuration in the stack.	SG
ping	Sends ICMP echo request packets to another node on the network.	UE
reload	Reloads the operating system.	PE
set description	Associates a text description with a switch in the stack.	SG
show boot-version	Displays the boot image version details.	UE
show cut-through mode	Show the cut-through mode on the switch.	PE
show memory cpu	Checks the total and available RAM space on the switch.	PE
show nsf	Shows non-stop forwarding status.	PE
show process cpu	Checks the CPU utilization for each process currently running on the switch.	PE
show sessions	Displays a list of the open telnet sessions to remote hosts.	PE
show stack-port	Displays summary stack-port information for all interfaces.	PE
show stack-port counters	Displays summary data counter information for all interfaces.	PE
show stack-port diag	Displays front panel stacking diagnostics for each port.	PE
show stack-standby	Shows the Standby configured in the stack.	UE
show supported switchtype	Displays information about all supported switch types.	UE
show switch	Displays information about the switch status.	UE
show system	Displays system information.	UE
show system id	Displays the service ID information.	UE
show tech-support	Displays system and configuration information (for debugging/calls to technical support).	PE
show users	Displays information about the active users.	PE

Command	Description	Mode*
show version	Displays the system version information.	UE
stack	Sets the mode to Stack Global Configuration mode.	GC
stack-port	Sets the mode to Stack Global Configuration mode to configure Stack ports as either Stacking ports or as Ethernet ports.	GC
standby	Configures the standby in the stack.	SG
switch priority	Configures the ability of the switch to become the Management Switch.	GC
switch renumber	Changes the identifier for a switch in the stack.	GC
telnet	Logs into a host that supports Telnet.	PE
traceroute	Discovers the IP routes that packets actually take when travelling to their destinations.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Telnet Server

Command	Description	Mode*
ip telnet server disable	Enables/disables the Telnet service on the switch.	GC
ip telnet port	Configures the Telnet service port number on the switch.	GC
show ip telnet	Displays the status of the Telnet server and the Telnet service port number.	PE
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

User Interface

Command	Description	Mode*
enable	Enters the privileged EXEC mode.	UE
end	Gets the CLI user control back to the privileged execution mode or user execution mode.	Any
exit(configuration)	Exits any configuration mode to the previously highest mode in the CLI mode hierarchy.	(All)
exit(EXEC)	Closes an active terminal session by logging off the switch.	UE
mode simple	Selects the simple mode as the start up mode.	GC
mode-change confirm	Confirms the mode selection.	GC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Web Server

Command	Description	Mode*
common-name	Specifies the common-name for the device.	CC
country	Specifies the country.	CC
crypto certificate generate	Generates a HTTPS certificate.	GC
crypto certificate import	Imports a certificate signed by the Certification Authority for HTTPS	GC
crypto certificate request	Generates and displays a certificate request for HTTPS	PE
duration	Specifies the duration in days.	CC
ip http port	Specifies the TCP port for use by a web browser to configure the switch.	GC
ip http server	Enables the switch to be configured from a browser.	GC
ip https certificate	Configures the active certificate for HTTPS	GC
ip https port	Configures a TCP port for use by a secure web browser to configure the switch.	GC

Command	Description	Mode*
ip https server	Enables the switch to be configured from a secured browser.	GC
key-generate	Specifies the key-generate.	CC
location	Specifies the location or city name.	CC
organization-unit	Specifies the organization-unit or department name	CC
show crypto certificate mycertificate	Displays the SSL certificates of your switch.	PE
show ip http	Displays the HTTP server configuration.	PE
show ip https	Displays the HTTPS server configuration.	PE
state	Specifies the state or province name.	CC
*NOTE: For the meaning of each Mode abbreviation, see "Mode Types" on page 64.		

Using the CLI

Introduction

This chapter describes the basics of entering and editing the Dell PowerConnect 62xx Series Command Line Interface (CLI) commands and defines the command hierarchy. It also explains how to activate the CLI and implement its major functions.

This chapter covers the following topics:

- Entering and Editing CLI Commands
- CLI Command Modes
- Starting the CLI
- Using CLI Functions and Tools

Entering and Editing CLI Commands

A CLI command is a series of keywords and arguments. Keywords identify a command and arguments specify configuration parameters. For example, in the command **show interfaces status ethernet 1/g5**, **show**, **interfaces** and **status** are keywords; **ethernet** is an argument that specifies the interface type, and **1/g5** specifies the unit/port.

When working with the CLI, the command options are not displayed. The command is not selected by a menu but is entered manually. To see what commands are available in each mode or within an Interface Configuration, the CLI provides a method of displaying the available commands, the command syntax requirements and in some instances parameters required to complete the command. The standard command to request context-sensitive help is the **<?>** key.

Two instances where the help information can be displayed are:

- **Keyword lookup** — The **<?>** key is entered in place of a command. A list of all valid commands and corresponding help messages is displayed.

- **Partial keyword lookup** — A command is incomplete and the <?> key is entered in place of a parameter. The matched parameters for this command are displayed.

The following features and conventions are applicable to CLI command entry and editing:

- History Buffer
- Negating Commands
- Show Command
- Command Completion
- Short Form Commands
- Keyboard Shortcuts
- Operating on Multiple Objects (Range)
- Command Scripting
- CLI Command Notation Conventions
- Interface Naming Conventions

History Buffer

Every time a command is entered in the CLI, it is recorded in an internally managed Command History buffer. Commands are stored in the buffer, which operates on a *First In First Out (FIFO)* basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved after switch resets.

Keyword	Source or Destination
Up-arrow key <Ctrl> + <P>	Recalls commands in the history buffer, beginning with the most recent command. Repeats the key sequence to recall successively older commands.
Down-arrow key <Ctrl> + <N>	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence recalls more recent commands in succession.

By default, the history buffer system is enabled, but it can be disabled at any time. The standard number of 10 stored commands can be increased to 216. By configuring 0, the effect is the same as disabling the history buffer system.

For information about the command syntax for configuring the command history buffer, see the **history-size** command in the Line command mode chapter of this guide.

Negating Commands

For many commands, the prefix keyword **no** is entered to cancel the effect of a command or reset the configuration to the default value. All configuration commands have this capability. This guide describes the negation effect for all commands to which it applies.

Show Command

The **show** command executes in the User Executive (EXEC) and Privileged Executive (EXEC) modes.

Command Completion

CLI can complete partially entered commands when the user presses the <tab> or <space> key. If a command entered is not complete, is not valid, or if some parameters of the command are not valid or missing, an error message is displayed to assist in entering the correct command. By pressing the <tab> key, an incomplete command is changed into a complete command. If the characters already entered are not enough for the system to identify a single matching command, the <?> key displays the available commands matching the characters already entered.

Short Form Commands

The CLI supports the short forms of all commands. As long as it is possible to recognize the entered command unambiguously, the CLI accepts the short form of the command as if the user typed the full command.

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The **help** command, when used in the User EXEC and Privileged EXEC modes, displays the keyboard short cuts.

The following table contains the CLI shortcuts displayed by the **help** command.

Keyboard Key	Description
<Delete, Backspace>	Delete previous character
<Ctrl> + <A>	Go to beginning of line
<Ctrl> + <E>	Go to end of line
<Ctrl> + <F>	Go forward one character
<Ctrl> + 	Go backward one character
<Ctrl> + <D>	Delete current character
<Ctrl> + <U,X>	Delete to beginning of line
<Ctrl> + <K>	Delete to the end of the line.
<Ctrl> + <W>	Delete previous word
<Ctrl> + <T>	Transpose previous character
<Ctrl> + <P>	Go to previous line history buffer
<Ctrl> + <R>	Rewrites or pastes the line
<Ctrl> + <N>	Go to next line in history buffer
<Ctrl> + <Y>	Print last deleted character
<Ctrl> + <Q>	Enables serial flow
<Ctrl> + <S>	Disables serial flow
<Ctrl> + <Z>	Return to root command prompt
<Tab, SPACE>	Command-line completion
end	Return to the root command prompt
exit	Go to next lower command prompt
<?>	List choices

Operating on Multiple Objects (Range)

The CLI allows the user to operate on the set of objects at the same time. The guidelines are as follows for range operation:

- Operations on objects with four or more instances support the range operation.
- The **range** key word is used to identify the range of objects on which to operate.

- The range may be specified in the following manner:
 (#-#) — a range from a particular instance to another instance (inclusive). For example, 1/g1-g10 indicates that the operation applies to the gigabit Ethernet ports 1 to 10 on unit 1.
 (#, #, #) — a list of non-consecutive instances. For example, (1/g1, 1/g3, 1/g5) indicates that the operation applies to the gigabit Ethernet ports 1, 3, and 5 on unit 1.
 (#, #-#, #) — ranges and non-consecutive instances listed together. For example, (1/g1, 1/g3-g5, 1/g7) indicates that the operation applies to the gigabit Ethernet ports 1, 7, and 3 to 5 on unit 1.



NOTE: Each # must be a fully qualified port identifier, that is, type<unit>/<port_type><port_number>, where unit is 1-12, port_type is g or xg and port_number is 1-24 or 1-48 in the case of port_type g and 1-4 for port_type xg. The following formats are allowed:(#-#,#), (#,#-#,#), (#,#-#,#-#,#). For LAG, use *"interface range port-channel 1-48"*.

- When operating on a range of objects, the CLI implementation hides the parameters that may not be configured in a range (for example, parameters that must be uniquely configured for each instance).
- The CLI uses best effort when operating on a list of objects. If the user requests an operation on a list of objects, the CLI attempts to execute the operation on as many objects in the list as possible even if failure occurs for some of the items in the list. The CLI provides the user with a detailed list of all failures, listing the objects and the reasons for the failures.
- Some parameters must be configured individually for each port or interface.

Command Scripting

The CLI can be used as a programmable management interface. To facilitate this function, any characters entered after the <!> character are treated as a comment and ignored by the CLI. Also, the CLI allows the user to disable session timeouts.

CLI Command Notation Conventions

When entering commands there are certain command-entry notations which apply to all commands. The following table describes these conventions as they are used in syntax definitions.

Convention	Description
[]	In a command line, square brackets indicate an optional entry.
{ }	In a command line inclusive brackets indicate a selection of compulsory parameters separated by the character. One option must be selected. For example: flowcontrol {auto on off} means that for the flowcontrol command either auto , on or off must be selected.
<i>Italic</i>	Indicates a variable.
<Enter>	Any individual key on the keyboard.
<Ctrl> + <F4>	Any combination of keys pressed simultaneously on the keyboard.
Screen Display	Indicates system messages and prompts appearing on the console.
all	Indicates a literal parameter, entered into the command as it is.

Interface Naming Conventions

The conventions for naming interfaces in CLI commands are as follows:

- Unit#/Interface ID — each interface is identified by the *Unit#* followed by a </> symbol and then the *Interface ID*. For example, *2/g10* identifies the gigabit port 10 within the second unit.
- Unit# — the unit number is used only in a stacking solution where a number of switches are stacked to form a virtual switch. In this case, the *Unit #* identifies the physical switch identifier within the stack.
- Interface ID — is formed by the interface type followed by the interface number. For example, *2/g10* identifies the gigabit port 10 on the second unit; *1/g1* identifies the fast Ethernet port 1 on the first unit within the stack.
- Interface Types — the following interface types are defined. *g* stands for gigabit Ethernet port (for example, *g2* is the gigabit port 2). *xg* stands for 10 Gigabit Ethernet port (for example, *xg2* is the 10 gigabit Ethernet port 2).

CLI Command Modes

Since the set of CLI commands is very large, the CLI is structured as a command-tree hierarchy, where related command sets are assigned to command modes for easier access. At each level, only the commands related to that level are available to the user and only those commands are shown in the context sensitive help for that level.

In this guide, commands are organized into three categories:

- Layer 2 (Data Link Layer) commands
- Layer 3 (Network Layer) commands
- Utility Commands

Layer 2 (Data Link Layer) describes the logical organization of data bits transmitted on a particular medium. This layer defines the framing, addressing and checksumming of Ethernet packets.

Layer 3 (Network Layer) describes how a series of exchanges over various data links can deliver data between any two nodes in a network. This layer defines the addressing and routing structure of the Internet.

Utility describes commands used to manage the switch.

Commands that cause specific actions to be taken immediately by the system and do not directly affect the system configurations are defined at the top of the command tree. For example, commands for rebooting the system or for downloading or backing up the system configuration files are placed at the top of the hierarchy tree.

Commands that result in configuration changes to the switch are grouped in a Configuration sub tree.

There are levels beneath the Configuration mode for further grouping of commands. The system prompt reflects these sub-Configuration modes.

All the parameters are provided with reasonable defaults where possible.

When starting a session, the initial mode is the User EXEC mode. Only a limited subset of commands is available in this mode. This level is reserved for tasks that do not change the configuration. To enter the next level, the Privileged EXEC mode, a password is required.

The Privileged EXEC mode provides access to commands that can not be executed in the User EXEC mode and permits access to the switch Configuration mode.

The Global Configuration mode manages switch configuration on a global level. For specific interface configurations, command modes exist at a sub-level.

Entering a `<?>` at the system prompt displays a list of commands available for that particular command mode. A specific command is used to navigate from one command mode to another. The standard order to access the modes is as follows: User EXEC mode, Privileged EXEC mode, Global Configuration mode, and Interface Configuration and other specific configuration modes.

User EXEC Mode

After logging into the switch, the user is automatically in the User EXEC command mode unless the user is defined as a privileged user. In general, the User EXEC commands allow the user to perform basic tests, and list system information.

The user-level prompt consists of the switch host name followed by the angle bracket (`>`).

```
console>
```

The default host name is Console unless it has been changed using the `hostname` command in the Global Configuration mode.

Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access is password-protected to prevent unauthorized use. The password is not displayed on the screen and is case sensitive.

Privileged users enter into the Privileged EXEC mode from User EXEC mode, where the following prompt is displayed.

```
console#
```

Global Configuration Mode

Global Configuration commands apply to features that affect the system as a whole, rather than just a specific interface. The Privileged EXEC mode command **configure** is used to enter the Global Configuration mode.

```
console (config) #
```

Interface and Other Specific Configuration Modes

Interface configuration modes are used to modify specific interface operations. The following are the Interface Configuration and other specific configuration modes:

- **MST** — The Global Configuration mode command **spanning-tree mst** configuration is used to enter into the Multiple Spanning Tree configuration mode.
- **Line Interface** — Contains commands to configure the management connections. These include commands such as line speed and timeout settings. The Global Configuration mode command **line** is used to enter the Line Interface mode.
- **VLAN Database** — Contains commands to create a VLAN as a whole. The Global Configuration mode command **vlan database** is used to enter the VLAN Database mode.
- **Router OSPF Configuration** — Global configuration mode command **router ospf** is used to enter into the Router OSPF Configuration mode.
- **Router RIP Configuration** — Global configuration mode command **router rip** is used to enter into the Router RIP Configuration mode.
- **Router OSPFv3 Configuration** — Global configuration mode command **ipv6 router ospf** is used to enter into the Router OSPFv3 Configuration mode.
- **IPv6 DHCP Pool Mode** — Global configuration mode command **ipv6 dhcp pool** is used to enter into the IPv6 DHCP Pool mode.
- **Management Access List** — Contains commands to define management access administration lists. The Global Configuration mode command **management access-list** is used to enter the Management Access List configuration mode.

- **Policy-map** — Use the **policy-map** command to access the QoS policy map configuration mode to configure the QoS policy map.
- **Policy Class** — Use the **class** command to access the QoS Policy-class mode to attach or remove a DiffServ class from a policy and to configure the QoS policy class.
- **Class-Map** — This mode consists of class creation/deletion and matching commands. The class matching commands specify layer 2, layer 3 and general match criteria. Use the class-map class-map-name commands to access the QoS Class Map Configuration mode to configure QoS class maps.
- **Stack** — Use the stack command to access the Stack Configuration Mode.
- **Ethernet** — Contains commands to manage Ethernet port configuration. The Global Configuration mode command **interface ethernet** enters the Interface Configuration mode to configure an Ethernet interface.
- **Port Channel** — Contains commands to configure port-channels, i.e., assigning ports to a port-channel. Most of these commands are the same as the commands in the Ethernet interface mode and are used to manage the member ports as a single entity. The Global Configuration mode command **interface port-channel** is used to enter the Port Channel mode.
- **Tunnel** — Contains commands to manage tunnel interfaces. The Global Configuration mode command **interface tunnel** enters the Tunnel Configuration mode to configure an tunnel type interface.
- **Loopback** — Contains commands to manage loopback interfaces. The Global Configuration mode command **interface loopback** enters the Loopback Configuration mode to configure an loopback type interface.
- **SSH Public Key-chain** — Contains commands to manually specify other switch SSH public keys. The Global Configuration mode command **crypto key pub-key chain ssh** is used to enter the SSH Public Key-chain configuration mode.
- **SSH Public Key-string** — Contains commands to manually specify the SSH Public-key of a remote SSH Client. The SSH Public-Key Chain Configuration mode command **user-key** command is used to enter the SSH Public-Key Configuration mode.

- **MAC Access-List** — Configures conditions required to allow traffic based on MAC addresses. The Global Configuration mode command **mac-access-list** is used to enter the MAC Access-List configuration mode.
- **TACACS** — Configures the parameters for the TACACS server.
- **Radius** — Configures the parameters for the RADIUS server.
- **SNMP Host Configuration** — Configures the parameters for the SNMP server host.
- **SNMP v3 Host Configuration** — Configures the parameters for the SNMP v3 server host.
- **SNMP Community Configuration** — Configures the parameters for the SNMP server community.
- **Crypto Certificate Request** — Configures the parameters for crypto certificate request.
- **Crypto Certificate Generation** — Configures the parameters for crypto certificate generate.
- **Logging** — Configures the parameters for syslog log server.

Identifying the Switch and Command Mode from the System Prompt

The system prompt provides the user with the name of the switch (hostname) and identifies the command mode. The following is a formal description of the system command prompt:

[device name][(*[command mode-[object]*)]][#|>]

[device name] — is the name of the managed switch, which is typically the user-configured hostname established by the **hostname** command.

[command mode] — is the current configuration mode and is omitted for the top configuration levels.

[object] — indicates specific object or range of objects within the configuration mode.

For example, if the current configuration mode is config-if and the object being operated on is gigabit ethernet 1 on unit 1, the prompt displays the object type and unit (for example, 1/g1).

[# | >] — The # sign is used to indicate that the system is in the Privileged EXEC mode. The > symbol indicates that the system is in the User EXEC mode, which is a read-only mode in which the system does not allow configuration.

Navigating CLI Command Modes

The following table describes how to navigate through the CLI Command Mode hierarchy.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
User EXEC	The user is automatically in User EXEC mode unless the user is defined as a privileged user.	console>	logout
Privileged EXEC	Use the enable command to enter into this mode. This mode is password protected.	console#	Use the exit command, or press <Ctrl>+<Z> to return to the User EXEC mode.
Global Configuration	From Privileged EXEC mode, use the configure command.	console (config) #	Use the exit command, or press <Ctrl>+<Z> to return to the Privileged EXEC mode.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Line Interface	From Global Configuration mode, use the line command.	console (config-line) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Management Access-List	From Global Configuration mode, use the management access-list command.	console (config-macal) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Policy-Class-Map	From Global Configuration mode, use the policy-map class command.	console (config-policy-classmap) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Class-Map	From Global Configuration mode, use the class-map command.	console (config-classmap) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
MAC Access List	From Global Configuration mode, use the mac access-list command.	<code>console (config-mac-access-list) #</code>	To exit to Global Configuration mode, use the exit command, or press <code><Ctrl> + <Z></code> to Privileged EXEC mode.
SSH Public Key-Chain	From Global Configuration mode, use the crypto key pubkey-chain ssh command.	<code>console (config-pubkey-chain) #</code>	To exit to Global Configuration mode, use the exit command, or press <code><Ctrl> + <Z></code> to Privileged EXEC mode.
SSH Public Key String	From the SSH Public Key-Chain mode, use the user-key <user name> {rsa dsa} command.	<code>console (config-pubkey-key) #</code>	To return to the SSH Public key-chain mode, use the exit command, or press <code><Ctrl> + <Z></code> to Privileged EXEC mode.
TACACS	From Global Configuration mode, use the tacacs-server host command.	<code>console (tacacs) #</code>	To exit to Global Configuration mode, use the exit command, or press <code><Ctrl> + <Z></code> to Privileged EXEC mode.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Radius	From Global Configuration mode, use the radius-server host command.	<code>console (config-radius) #</code>	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
SNMP Host Configuration	From Global Configuration mode, use the snmp-server command.	<code>console (config-snmp) #</code>	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
SNMP v3 Host Configuration	From Global Configuration mode, use the snmp-server v3-host command.	<code>console (config-snmp) #</code>	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
SNMP Community Configuration	From Global Configuration mode, use the snmp-server community command.	<code>console (config-snmp) #</code>	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Crypto Certificate Generation	From Global Configuration mode, use the crypto certificate <i>number</i> generate command.	console (config-crypto-cert) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Crypto Certificate Request	From Privileged EXEC mode, use the crypto certificate <i>number</i> request command.	console (config-crypto-cert) #	To exit to Privileged EXEC mode, use the exit command, or press <Ctrl> + <Z>.
Stack	From Global Configuration mode, use the stack command.	console (config-stack) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Logging	From Global Configuration mode, use the logging command.	console (config-logging) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
MST	From Global Configuration mode, use the spanning-tree mst configuration command.	console (config-mst) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
VLAN Config	From Global Configuration mode, use the vlan database command.	console (config-vlan) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Router OSPF Conf	From Global Configuration mode, use the router ospf command.	console (config-router) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode
Router RIP Config	From Global Configuration mode, use the router rip command.	console (config-router) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
Router OSPFv3 Config	From Global Configuration mode, use the ipv6 router ospf command.	console (config-rtr) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode
IPv6 DHCP Pool Mode	From Global Configuration mode, use the ipv6 dhcp pool command.	console (config-dhcp6s-pool) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode
Interface Configuration Modes			
Ethernet	From Global Configuration mode, use the interface ethernet command.	console (config-if-n/gn or n/xgn) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Port Channel	From Global Configuration mode, use the interface port-channel command.	console (config-if-chn) #	To exit to Global Configuration mode, use the exit command, or <Ctrl> + <Z> to Privileged EXEC mode.

Command Mode	Access Method	Command Prompt	Exit or Access Previous Mode
VLAN	From Global Configuration mode, use the interface vlan command.	console (config-if-vlann) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Tunnel	From Global Configuration mode, use the interface tunnel command.	console (config-tunneln) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.
Loopback	From Global configuration mode, use the interface loopback command.	console (config-loopbackn) #	To exit to Global Configuration mode, use the exit command, or press <Ctrl> + <Z> to Privileged EXEC mode.

Starting the CLI

To begin running the CLI, perform the following steps:



NOTE: This procedure is for use on the console line only.



NOTE: The Easy Setup Wizard is available only when the system is in default state with no user configuration saved previously.

- 1 Start the switch and wait until the startup procedure is complete and the User EXEC mode is entered. The prompt *console>* is displayed.
- 2 Configure the switch using the Easy Setup Wizard and enter the necessary commands to complete the required tasks.
- 3 When finished, exit the session with the **quit** or **exit** command.

The switch can be managed over a direct connection to the switch console port or through a Telnet connection. If access is through a Telnet connection, the switch must have a defined IP address, corresponding management access granted, and a connection to the network.

Easy Setup Wizard

The Easy Setup Wizard guides the user in the basic initial configuration of a newly installed switch so that it can be immediately deployed and functional in its basic operation and be completely manageable through the Web, CLI and the remote Dell Network Manager. After initial setup, the user may enter to the system to set up more advanced configurations.

By default the switch is shipped from the factory with an IP address of 192.168.2.1 but the Easy Setup Wizard provides the opportunity to customize the IP address. Also the system is set up with default management VLAN ID=1. The initial activation must be done using the serial interface since, without a unique IP address, the user can not access the other management interfaces.

The wizard sets up the following configuration on the switch:

- Establishes the initial privileged user account with a valid password. The wizard configures one privileged user account during the setup. The user may return to add users later. The initial account is given the highest privilege level (level 15).

- Enables CLI login and HTTP access to use the local authentication setting only, which allows user account access via these management interfaces. The user may return later to configure Radius or TACACS+.
- Sets up the IP address for the management VLAN or enables support for DHCP to configure the management IP address dynamically.
- Sets up the SNMP community string to be used by the SNMP manager. The user may choose to skip this step if SNMP management is not used. If it is configured, the default access level is set to the highest available access for the SNMP management interface. The user may return later to add to the community string or reconfigure the access level of the community string. Initially only SNMPv1/2c will be activated. SNMPv3 is disabled until the user returns to configure security access for SNMPv3 (for example, engine ID, view, and so on). The SNMP community string may include spaces. The wizard requires the use of quotation marks when the user wants to enter spaces in the community string. Although spaces are allowed in the community string, their use is discouraged. The default community string contains no spaces.
- Allows the user to specify the management server IP or permit SNMP access from all IP addresses.
- Sets up the default gateway IP address.

If the user chooses not to use the wizard initially, the session defaults to the CLI mode with a warning to refer the documentation. During a subsequent login, the user may again elect not to run the setup wizard. Once the wizard has established configuration, however, the wizard is presented only if the user resets the switch to the factory default settings. While the wizard is running, the system does not display any unsolicited or unrelated status messages. For example, the system does not display event notification or system status messages.

After completing the wizard, the user is given a chance to save his configuration and continue to the CLI. If the user chooses to discard his configuration, any restart of the wizard must be from the beginning. When the user chooses to restart the wizard, any configuration the user saved previously automatically is offered for the user to accept. The user may elect to correct only a few items instead of re-entering all the data.

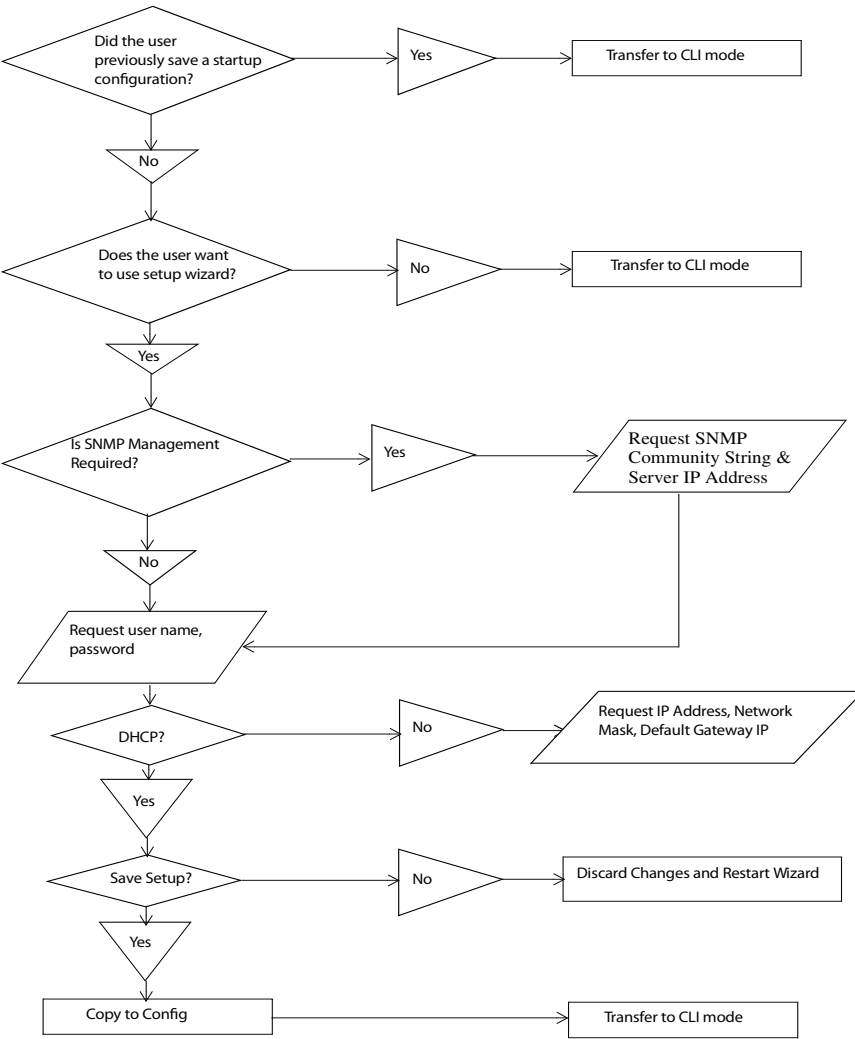
Since a switch may be powered on in the field without a serial connection, the switch waits 60 seconds for the user to respond to the setup wizard question in instances where no configuration files exist. If there is no response, the switch continues normal operation using the default factory configuration. While waiting for the response from the user, normal switch operation will continue, including but not limited to:

- If BOOTP/DHCP is supported and enabled by default, the switch attempts to get its address.
- The switch continues to switch traffic.
- The switch continues to do MAC learning. If spanning-tree is on by default, the switch participates in the spanning-tree protocol.

Functional Flow

The functional flow diagram in Figure 2-1 illustrates the procedures for the Easy Setup Wizard.

Figure 2-1. Easy Setup Wizard



Example Session

This section describes an Easy Setup Wizard session. Refer to the state diagram in the previous section for general flow. The following values used by the example session are not the only possible ones:

- IP address for the management VLAN is 192.168.2.1;255.255.255.0.
- The user name is *admin*, and the password should be 8-64 characters in length (admin123).
- The network management system IP address is 192.168.2.1.
- The default gateway is 0.0.0.0.
- The SNMP community string to be used is *{public}*.

The setup wizard configures the initial values as defined above. After the user completes the wizard, the system is configured as follows:

- SNMPv1/2c is enabled and the community string is set up as defined above. SNMPv3 is disabled.
- The admin user account is set up as defined.
- A network management system is configured. From this management station, the user can access the SNMP, HTTP, and CLI interfaces. The user may also choose to allow all IP addresses to access these management interfaces by choosing the (0.0.0.0) IP address.
- An IP address is configured for the default management VLAN (1).
- A default gateway address is configured.

The following example contains the sequence of prompts and responses associated with running an example Dell Easy Setup Wizard session, using the input values listed above. Note in this case a static IP address for the management interface is being set up. However it may be requested that the system automatically retrieve an IP address via DHCP. If DHCP is used, the system does not request a network mask or default gateway. In this example, the user employs the setup wizard to configure the initial values as defined above.



NOTE: In the example, the possible user options are enclosed in []. Also, where possible, default values are enclosed in []. If the user enters <Return> with no options defined, the default value is accepted. Help text is in parentheses.

After the switch completes the POST and is booted, the following dialog appears:

Welcome to Dell Easy Setup Wizard

The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip the setup wizard, and enter CLI mode to manually configure the switch. You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation using the default system configuration. Note: You can exit the setup wizard at any point by entering [ctrl+z].

Would you like to run the setup wizard (you must answer this question within 60 seconds)? [Y/N] y

Step 1:

The system is not setup for SNMP management by default. To manage the switch using SNMP (required for Dell Network Manager) you can:

- o Set up the initial SNMP version 2 account now.
- o Return later and setup other SNMP accounts. (For more information on setting up an SNMP version 1 or 3 account, see the user documentation).

Would you like to setup the SNMP management interface now? [Y/N] y

To setup the SNMP management account you must specify the management system IP address and the "community string" or password that the particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to this account. You can use Dell Network Manager or other management interfaces to change this setting, and to add additional management system later. For more information on adding management systems, see the user documentation.

To add a management station:

Please enter the SNMP community string to be used.

{public}:

public<Enter>

Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station.

{0.0.0.0}:

192.168.2.1<Enter>

Step 2:

Now we need to setup your initial privilege (Level 15) user account. This account is used to login to the CLI and Web interface. You may setup other accounts and change privilege levels later. For more information on setting up user accounts and changing privilege levels, see the user documentation.

To setup a user account:

Please enter the user name: admin<Enter>

Please enter the user password: *****<Enter>

Please reenter the user password: *****<Enter>

Step 3:

Next, an IP address is setup. The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch.

Optionally you may request that the system automatically retrieve an IP address from the network via DHCP (this requires that you have a DHCP server running on the network).

To setup an IP address:

Please enter the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotes) to automatically request an IP address from the network DHCP server.

192.168.2.1<Enter>

Please enter the IP subnet mask (A.B.C.D or /nn):

255.255.255.0<Enter>

Step 4:

Finally, set up the gateway. Please enter the IP address of the gateway from which this network is reachable

192.168.1.1<Enter>

This is the configuration information that has been collected:

SNMP Interface = "public"@192.168.2.1

User Account setup = admin

Password = *****

Management IP address = 192.168.2.1 255.255.255.0

Gateway = 0.0.0.0

Step 5:

If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the information is incorrect, select (N) to discard configuration and restart the wizard: [Y/N]

y<Enter>

Thank you for using the Dell Easy Setup Wizard. You will now enter CLI mode.

.....

console>

Unit 1 - Waiting to select management unit)>

Applying configuration, please wait ...

Welcome to Dell Easy Setup Wizard

The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip the setup wizard, and enter CLI mode to manually configure the switch. You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation using the default system configuration. Note: You can exit the setup wizard at any point by entering [ctrl+z].

Would you like to run the setup wizard (you must answer this question within 60 seconds)? [Y/N] y

Step 1:

The system is not setup for SNMP management by default. To manage the switch using SNMP (required for Dell Network Manager) you can

- . Set up the initial SNMP version 2 account now.

- . Return later and setup other SNMP accounts. (For more information on setting up an SNMP version 1 or 3 account, see the user documentation).

Would you like to setup the SNMP management interface now? [Y/N] n

Step 2:

Now we need to setup your initial privilege (Level 15) user account. This account is used to login to the CLI and Web interface. You may setup other accounts and change privilege levels later. For more information on setting up user accounts and changing privilege levels, see the user documentation.

To setup a user account:

Please enter the user name. [root]:root

Please enter the user password:

Please reenter the user password:

Step 3:

Next, an IP address is setup. The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch. Optionally you may request that the system automatically retrieve an IP address from the network via DHCP (this requires that you have a DHCP server running on the network).

To setup an IP address:

Please enter the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotes) to automatically request an IP address from the network DHCP server.
[192.168.2.1]:

Please enter the IP subnet mask (A.B.C.D or /nn).
[255.255.255.0]:

Step 4:

Finally, setup the default gateway. Please enter the IP address of the gateway from which this network is reachable. [0.0.0.0]:

This is the configuration information that has been collected:

User Account setup = root

Password = *****

Management IP address = 192.168.2.1 255.255.255.0

Default Gateway = 0.0.0.0

Operation Mode = Normal

Step 5:

Do you want to select the operational mode as Simple Mode? [Y/N] n

Step 6:

If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the information is incorrect, select (N) to discard configuration and restart the wizard: [Y/N]

Using CLI Functions and Tools

The CLI has been designed to manage the switch's configuration file system and to manage switch security. A number of resident tools exist to support these and other functions.

Configuration Management

All managed systems have software images and databases that must be configured, backed up and restored. Two software images may be stored on the system, but only one of them is active. The other one is a backup image. The same is true for configuration images, which store the configuration parameters for the switch. The system has three configuration images. One image is a memory-only image and is the current configuration image for the switch. The second image is the one that is loaded by the system when it reboots. There is one backup configuration image. The system also provides methods to back up these images to a remote system.

File System Commands

All files are stored in a flat file system. The following commands are used to perform operations on these files.

Command	Description
delete <i>file</i>	Deletes file.
filedescr <i>file description</i>	Adds a description to a file (up to 20 characters can be used).
copy <i>source destination</i>	Copies a file from source file to destination file.

Copying Files

The copy command not only provides a method for copying files within the file system, but also to and from remote servers. With the copy command and URLs to identify files, the user can back up images to local or remote systems or restore images from local or remote systems.

To use the copy command, the user specifies the source file and the destination file. For example, copy *http://remotehost/pub/backupfile backup-config* copies a file from the remote TFTP server to a local backup

configuration file. In this case, if the local configuration file does not exist, then it is created by the command. If it does exist, it is overwritten. If there is not enough space on the local file system to accommodate the file, an error is flagged.

Refer to the **copy** command description in the Layer 2 commands section of the guide for command details.

Referencing External/Internal File systems

Configuration or software images are copied to or retrieved from remote file systems using TFTP and XMODEM protocols.

- `tftp://server-name/path/filename` — identifies a file on a remote file system accessible through the `server-name`. Trivial file transfer protocol is a simplified FTP and uses a UDP port instead of TCP and does not have password protection.
- `xmodem: filename` — identifies the file available on the XMODEM connection.

Special System Files

The following special filenames are used to refer to special virtual system files, which are under control of the system and may not be removed or added. These file names are reserved and may not be used as user-defined files. When the user copies a local source file into one of these special files and the source file has an attached file description, it also is copied as the file description for the special file.

- **backup-config** — This file refers to the backup configuration file.
- **running-config** — This file refers to the configuration file currently active in the system. It is possible to copy the `running-config` image to a `backup-config` file or to the `startup-config` file.
- **startup-config** — This file refers to the special configuration image stored in flash memory which is loaded when the system next reboots. The user may copy a particular configuration file (remote or local) to this special file name and reboot the system to force it to use a particular configuration.
- **image1 & image2** — These files refer to software images. One of these will be loaded when the system next reboots. Either `image1` or `image2` can be chosen for the next reboot using the command **boot system**.

CLI prevents the user from accidentally copying a configuration image onto a software image and vice versa.

Management Interface Security

This section describes the minimum set of management interface security measures implemented by the CLI. Management interface security consists of user account management, user access control and remote network/host access controls.

CLI through Telnet, SSH, Serial Interfaces

The CLI is accessible through a local serial interface, a remote telnet, or secure shell sessions. Since the serial interface requires a physical connection for access, it is used if all else fails. The serial interface is the only interface from which the user may access the Easy Setup Wizard. It is the only interface that the user can access if the remote authentication servers are down and the user has not configured the system to revert to local managed accounts.

The following rules and specifications apply to these interfaces:

- The CLI is accessible from remote telnet through the management IP address for the switch.
- The CLI is accessible from a secure shell interface.
- The CLI generates keys for SSH locally.
- The serial session defaults to 9600 baud rate, eight data bits, non-parity and one stop bit.

User Accounts Management

The CLI provides authentication for users either through remote authentication servers supporting TACACS+ or Radius or through a set of locally managed user accounts. The setup wizard asks the user to create the initial administrator account and password at the time the system is booted.

The following rules and specifications apply:

- The user may create as many as five local user accounts.
- User accounts have an access level, a user name, and a user password.
- The user is able to delete the user accounts but the user will not be able to delete the last level 15 account.

- The user password is saved internally in encrypted format and never appears in clear text anywhere on the CLI.
- The CLI supports TACACS+ and Radius authentication servers.
- The CLI allows the user to configure primary and secondary authentication servers. If the primary authentication server fails to respond within a configurable period, the CLI automatically tries the secondary authentication server.
- The user can specify whether the CLI should revert to using local user accounts when the remote authentication servers do not respond or if the CLI simply fails the login attempt because the authentication servers are down. This requirement applies only when the user is login through a telnet or an SSH session.
- The CLI always allows the user to log in to a local serial port even if the remote authentication server(s) are down. In this case, CLI reverts to using the locally configured accounts to allow the user to log in.

User Access Control

In addition to authenticating a user, the CLI also assigns the user access to one of two security levels. Level 1 has read-only access. This level allow the user to read information but not configure the switch. The access to this level cannot be modified. Level 15 is the special access level assigned to the superuser of the switch. This level has full access to all functions within the switch and can not be modified.

If the user account is created and maintained locally, each user is given an access level at the time of account creation. If the user is authenticated through remote authentication servers, the authentication server is configured to pass the user access level to the CLI when the user is authenticated. When Radius is used, the *Vendor-Specific Option* field returns the access level for the user. Two vendor specific options are supported. These are CISCO-AV-Pairs(Shell:priv-lvl=x) and Dell Radius VSA (user-group=x). TACACS+ provides the appropriate level of access.

The following rules and specifications apply:

- The user determines whether remote authentication servers or locally defined user authentication accounts are used.

- If authentication servers are used, the user can identify at least two remote servers (the user may choose to configure only one server) and what protocol to use with the server, TACACS+ or Radius. One of the servers is primary and the other is the secondary server (the user is not required to specify a secondary server). If the primary server fails to respond in a configurable time period, the CLI automatically attempts to authenticate the user with the secondary server.
- The user is able to specify what happens when both primary and secondary servers fail to respond. In this case, the user is able to indicate that the CLI should either use the local user accounts or reject all requests.
- Even if the user configures the CLI to fail login when the remote authentication servers are down, the CLI allows the user to log in to the serial interface authenticated by locally managed account data.

Syslogs

The CLI uses syslog support to send logging messages to a remote syslog server. The user configures the switch to generate all logging messages to a remote log server. If no remote log server exists, then the CLI maintains a rolling log of at most the last 1000 critical system events.

The following rules and specifications apply:

- The CLI permits the user to configure a remote syslog server to which all system logging messages are sent.
- Log messages are implementation-dependent but may contain debug messages, security or fault events.
- If a log server is not specified by the user, the CLI maintains at most the last 1000 critical system events. In this case, less important events are not recorded.

Security Logs

Security logs are maintained to record all security events including the following:

- User login.
- User logout.
- Denied login attempts.
- User attempt to exceed security access level.

- Denied attempts by external management system to access the system.

The security log record contains the following information:

- The user name, if available, or the protocol being accessed if the event is related to a remote management system.
- The IP address from which the user is connecting or the IP address of the remote management system.
- A description of the security event.
- A timestamp of the event

If syslog is available, the CLI sends the security log records to the syslog server. If syslog is not available, the CLI records the last 1000 security log records in a log separate from the system log records itemized above. Also in this case, the CLI suppresses repeated events from the same source and instead the CLI records one event within a period of time and includes that count as part of the log.

Management ACL

In addition to user access control, the system also manages the access level for particular management interfaces. The system allows individual hosts or subnets to access only specific management protocols.

The user defines a management profile, which identifies management protocols such as the following:

- Telnet.
- SSH and the keying information to use for SSH.
- HTTP
- HTTPS and the security certificate to be used.
- SNMPv1/v2c and the read and read/write community strings to be used.
- SNMPv3 and the security information for used this protocol.

For each of these management profiles, the user defines the list of hosts or subnets from which the management profiles may be used.

Other CLI Tools and Capabilities

The CLI has several other capabilities associated with its primary functions.

Terminal Paging

The terminal width and length for CLI displays is 79 characters and 25 lines, respectively. The length setting is used to control the number of lines the CLI will display before it pauses. For example, the CLI pauses at 24 lines and prompts the user with the *-more-* prompt on the 25th line. The CLI waits for the user to press either <q> or any other key. If the user presses any key except <q>, the CLI shows the next page. A <q> key stops the display and returns to the CLI prompt.

Boot Message

The boot message is a system message that is not user-configurable and is displayed when the system is booting. Displayed information includes the following:

- Operational code date
- The board type
- The CPU
- Memory size

To start the normal booting process, select item 1 in the Boot Menu. The following is a sample log for booting information.

```
Boot Menu 3.2.0.1
```

```
CPU Card ID:    0x508541
```

```
/DskVol// - disk check in progress ...
```

```
/DskVol// - Volume is OK
```

```
total # of clusters:  15,147
```

```
# of free clusters:   5,299
```

```
# of bad clusters:    0
```

```
total free space:     10,598 Kb
```

```
max contiguous free space: 8,345,600 bytes
```

```
# of files:           30
```

```
# of folders:         1
```

```
total bytes in files: 19,656 Kb
# of lost chains: 0
total bytes in lost chains: 0

volume descriptor ptr (pVolDesc): 0x38ff9d0
XBD device block I/O handle: 0x10001
auto disk check on mount: DOS_CHK_REPAIR
|DOS_CHK_VERB_2
volume write mode: copyback (DOS_WRITE)
max # of simultaneously open files: 52
file descriptors in use: 0
# of different files in use: 0
# of descriptors for deleted files: 0
# of obsolete descriptors: 0
```

current volume configuration:

- volume label: NO LABEL ; (in boot sector:)
- volume Id: 0x1b19
- total number of sectors: 60,716
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 60
- # of FAT table copies: 2
- # of hidden sectors: 4

- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
- directory structure: VFAT
- file name format: 8-bit (extended-ASCII)
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240

FAT handler information:

- allocation group size: 2 clusters
- free space on volume: 10,852,352 bytes

Boot Menu 3.2.0.1

Select an option. If no selection in 10 seconds then operational code will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):

Operational Code Date: Mon Jan 4 04:26:56 2010

Uncompressing.....

Adding 0 symbols for standalone.

CPU: Motorola E500 : Unknown system version.
Processor #0.

Memory Size: 0x10000000. BSP version 1.2/0.

Created: Jan 4 2010, 03:59:27

ED&R Policy Mode: deployed

/DskVol// - disk check in progress ...

dosChkLib : CLOCK_REALTIME is being reset to TUE JUN
28 14:29:04 2005

Value obtained from file system volume descriptor
pointer: 0x348ef70

The old setting was THU JAN 01 00:00:00 1970

Accepted system dates are greater than THU DEC 27
00:00:00 1990

/DskVol// - Volume is OK

total # of clusters: 15,147

of free clusters: 5,299

of bad clusters: 0

total free space: 10,598 Kb

max contiguous free space: 8,345,600 bytes

of files: 30

of folders: 1

total bytes in files: 19,656 Kb

of lost chains: 0

total bytes in lost chains: 0

```

volume descriptor ptr (pVolDesc):      0x348ef70
XBD device block I/O handle: 0x10001
auto disk check on mount:      DOS_CHK_REPAIR
|DOS_CHK_VERB_2
volume write mode:      copyback (DOS_WRITE)
max # of simultaneously open files:      52
file descriptors in use:      0
# of different files in use:      0
# of descriptors for deleted files:      0
# of obsolete descriptors:      0

current volume configuration:
- volume label:      NO LABEL ; (in boot sector:
)
- volume Id:      0x1b19
- total number of sectors:      60,716
- bytes per sector:      512
- # of sectors per cluster: 4
- # of reserved sectors:      1
- FAT entry size:      FAT16
- # of sectors per FAT copy:      60
- # of FAT table copies:      2
- # of hidden sectors:      4
- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
- directory structure:      VFAT

```

- file name format: 8-bit (extended-ASCII)
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240

FAT handler information:

- allocation group size: 2 clusters
- free space on volume: 10,852,352 bytes

Timebase: 66.666666 MHz, MEM: 266.666664 MHz, PCI:
66.666666 MHz, CPU: 533.333328 MHz

PCI unit 0: Dev 0xb314, Rev 0x01, Chip BCM56314_A0,
Driver BCM56314_A0

SOC unit 0 attached to PCI device BCM56314_A0

Adding BCM transport pointers

Configuring CPUTRANS TX

Configuring CPUTRANS RX

Instantiating /download as rawFs, device = 0x20001

Formatting /download for DOSFS

Instantiating /download as rawFs, device = 0x20001

Formatting.../download: file system is marked clean,
skipping check

OK.

```
<186> JUN 28 14:29:09 0.0.0.0-1 UNKN[268434720]:  
bootos.c(222) 1 %% Event(0xaaaaaaaa)
```

```
Instantiating RamCP: as rawFs, device = 0x30001
```

```
Formatting RamCP: for DOSFS
```

```
Instantiating RamCP: as rawFs, device = 0x30001
```

```
RamCP:/ - disk check in progress ...
```

```
RamCP:/ - Volume is OK
```

```
total # of clusters: 1,975
```

```
# of free clusters: 1,973
```

```
# of bad clusters: 0
```

```
total free space: 1,010,176
```

```
max contiguous free space: 1,010,176 bytes
```

```
# of files: 0
```

```
# of folders: 0
```

```
total bytes in files: 0
```

```
# of lost chains: 0
```

```
total bytes in lost chains: 0
```

```
OK.
```

```
(Unit 1 - Waiting to select management unit)>
```

```
Welcome to Dell Easy Setup Wizard
```

```
The Setup Wizard guides you through the initial switch  
configuration, and
```

gets you up and running as quickly as possible. You can skip the setup wizard, and enter CLI mode to manually configure the switch. You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation using the default system configuration. Note: You can exit the setup wizard at any point by entering [ctrl+z].

Would you like to run the setup wizard (you must answer this question within

60 seconds)? [Y/N] n

Thank you for using Dell Easy Set up Wizard. You will now enter CLI mode.

Applying Global configuration, please wait ...

Applying Interface configuration, please wait ...

console>

console>

console>

console>show switch

SW	Management Status	Standby Status	Preconfig Model ID	Plugged-in Model ID	Switch Status	Code Version
1	Mgmt Sw		PC6224	PCT6224	OK	3.2.1.3

console>

Boot Utility Menu

If a user is connected through the serial interface during the boot sequence, pressing the <esc> key interrupts the boot process and displays a Boot Utility Menu. Selecting item 2 displays the menu and may be typed only during the initial boot up sequence. When the system boot up is complete, typing the escape sequence *does not* display the menu.

Reloading all switches.

Boot code.....

Boot Menu Version: 3.2.0.1

Select an option. If no selection in 10 seconds then operational code will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):2

The Boot Utility Menu offers the following options:

- 1 - Start operational code
- 2 - Change baud rate
- 3 - Retrieve event log using XMODEM
- 4 - Load new operational code using XMODEM
- 5 - Display operational code vital product data
- 6 - Abort code update
- 7 - Update boot code

- 8 - Delete backup image
- 9 - Reset the system
- 10 - Restore Configuration to factory defaults
(delete config files)
- 11 - Activate Backup Image
- 12 - Password Recovery Procedure

The boot utility menu provides the following:

- Option to set baud rate of the serial port.

[Boot Menu] 2

Select baud rate:

- 1 - 1200
- 2 - 2400
- 3 - 4800
- 4 - 9600
- 5 - 19200
- 6 - 38400
- 7 - 57600
- 8 - 115200
- 0 - no change

The previously described setting takes effect immediately.

- Option to retrieve event log using XMODEM.

[Boot Menu] 3

Sending event log, start XMODEM receive.....

- Option to load new operational code using XMODEM

[Boot Menu] 4

Ready to receive the file with XMODEM/CRC....

Ready to RECEIVE File xcode.bin in binary mode

Send several Control-X characters to cancel before transfer starts.

- Option to display Boot Image Information. This option can be used to determine which image is active and will be booted when option one is chosen.

[Boot Menu] 5

The following image is in the Flash File System:

File

Name.....image2

CRC.....0x
dd0a (56586)

Target

Device.....0x0050854
1

Size.....0x
91ced4 (9555668)

Number of Components.....3

Operational Code

Size.....0x790208 (7930376)

Operational Code

Offset.....0x74 (116)

Operational Code FLASH flag.....1

Operational Code

CRC.....0x9EBE

Operational Compression flag.....2
(lzma)

Boot Code Version.....1

Boot Code
Size.....0x100000
(1048576)

Boot Code
Offset.....0x79027c
(7930492)

Boot Code FLASH flag.....0

Boot Code
CRC.....0x2C8B

VPD - rel 3 ver 2 maint_lvl 0 build_num 1

Timestamp - Mon Jan 4 04:26:56 2010

File - Dell-Ent-esw-kinnick-pct.8541-V6R-
CSxw-6IQHSr3v2m0b1.opr

- Option to Abort boot code update

[Boot Menu] 6

There is no output from this option.

- Option to Update Boot Code.

[Boot Menu] 7

This is the output from the update boot code option:

Do you wish to update Boot Code? (y/n) y

Validating image2....OK

Extracting boot code from image...CRC valid

Erasing Boot Flash.....^^^^Done.

Wrote 0x10000 bytes.

Wrote 0x20000 bytes.

Wrote 0x30000 bytes.

Wrote 0x40000 bytes.

Wrote 0x50000 bytes.

Wrote 0x60000 bytes.

Wrote 0x70000 bytes.

Wrote 0x80000 bytes.

Wrote 0x90000 bytes.

Wrote 0xa0000 bytes.

Wrote 0xb0000 bytes.

Wrote 0xc0000 bytes.

Wrote 0xd0000 bytes.

Wrote 0xe0000 bytes.

Wrote 0xf0000 bytes.

Wrote 0x100000 bytes.

Validating Flash.....Passed

Flash update completed.

- Option to Delete backup image. The user is not allowed to delete active image.

[Boot Menu] 8

Are you SURE you want to delete backup code :
image2 ? (y/n):

- Option to Clear All Flash and Reset the System to Default Setting. User action will be confirmed with a Y/N question before executing the command. The following is the procedure to reset the system through Boot Menu:

```
[Boot Menu] 9
```

```
Are you SURE you want to reset the system? (y/n):y
```

```
Boot code.....
```

```
Boot Menu Version: 3.2.0.1
```

```
Select an option. If no selection in 10 seconds  
then operational code will  
start.
```

```
1 - Start operational code.
```

```
2 - Start Boot Menu.
```

```
Select (1, 2):2
```

- Option to Boot Without Using Startup Configuration and Only Load System Default. Selecting 10 from the Boot Menu restores system defaults. The boot sequence is started by selecting '1' from Boot Menu.

```
[Boot Menu] 10
```

```
Are you SURE you want to delete the startup-  
config? (y/n):
```

- Option To Activate the Backup Image. This option determines the active image and toggle the bootloader to use the backup image.

```
[Boot Menu] 11
```

```
Backup image - image1 activated.
```

- Option to use the password recovery procedure. It allows the switch to boot one time without prompting for a console password. Note that the ‘enable’ password is not prompted for in this mode.

[Boot Menu] 12

Monitoring Traps from CLI

It is possible to connect to the CLI session and monitor the events or faults that are being sent as traps from the system. This feature is equivalent to the alarm-monitoring window in a typical network management system. The user enables events or monitor traps from the CLI by entering the command **logging console**. Traps generated by the system are dumped to all CLI sessions that have requested monitoring mode to be enabled. The **no logging console** command disables trap monitoring for the session. By default, console logging is enabled.

AAA Commands

This chapter explains the following commands:

- `aaa authentication dot1x`
- `aaa authentication enable`
- `aaa authentication login`
- `aaa authorization network default radius`
- `enable authentication`
- `enable password`
- `ip http authentication`
- `ip https authentication`
- `login authentication`
- `password (Line Configuration)`
- `password (User EXEC)`
- `show authentication methods`
- `show users accounts`
- `show users login-history`
- `username`

aaa authentication dot1x

Use the `aaa authentication dot1x` command in Global Configuration mode to create an authentication login list.

Syntax

`aaa authentication dot1x default method1`

`no aaa authentication dot1x default`

- method1* — At least one from the following table:

Keyword	Description
radius	Uses the list of all authentication servers for authentication
none	Uses no authentication

Default Configuration

No authentication method is defined.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following example uses the `aaa authentication dot1x default` command with no authentication.

```
console(config)# aaa authentication dot1x default
none
```


aaa authentication enable

Use the **aaa authentication enable** command in Global Configuration mode to set authentication for accessing higher privilege levels. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication enable {default | *list-name*} *method1* [*method2*...]

no aaa authentication enable {default | *list-name*}

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
- *list-name* — Character string used to name the list of authentication methods activated, when using access higher privilege levels. (Range: 1-12 characters)
- *method1* [*method2*...] — Specify at least one from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The default enable list is "enableList." It is used by console, telnet, and SSH and only contains the method *none*.

Command Mode

Global Configuration mode

User Guidelines

The default and optional list names created with the **aaa authentication enable** command are used with the **enable authentication** command.

Create a list by entering the **aaa authentication enable *list-name method*** command where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. Note that **enable** will not succeed for a level one user if no authentication method is defined. A level one user must authenticate to get to privileged EXEC mode. For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.



NOTE: Requests sent by the switch to a RADIUS server include the username "\$enabx\$", where x is the requested privilege level. For enable to be authenticated on Radius servers, add "\$enabx\$" users to them. The login user ID is now sent to TACACS+ servers for enable authentication.

Example

The following example sets authentication when accessing higher privilege levels.

```
console(config)# aaa authentication enable default  
enable
```

aaa authentication login

Use the **aaa authentication login** command in Global Configuration mode to set authentication at login. To return to the default configuration, use the **no** form of this command.

Syntax

aaa authentication login {default | *list-name*} *method1* [*method2*...]

no aaa authentication login {default | *list-name*}

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
- *list-name* — Character string used to name the list of authentication methods activated when a user logs in. (Range: 1-12 characters)

- *method1* [*method2...*] — Specify at least one from the following table:

Keyword	Source or destination
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The default login lists are "defaultList" and "networkList." "defaultList" is used by the console and only contains the method *none*. "networkList" is used by telnet and SSH and only contains the method *local*.

Command Mode

Global Configuration mode

User Guidelines

The default and optional list names created with the **aaa authentication login** command are used with the **login authentication** command. Create a list by entering the **aaa authentication login list-name method** command for a particular protocol, where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

Example

The following example configures authentication login.

```
console(config)# aaa authentication login default
radius local enable none
```

aaa authorization network default radius

Use the **aaa authorization network default radius** command in Global Configuration mode to enable the switch to accept VLAN assignment by the RADIUS server.

Syntax

aaa authorization network default radius

no aaa authorization network default radius

- **default** — Name of the authorization list
- **radius** — Name of the authorization method

Default Configuration

By default, the switch does not accept VLAN assignments by the RADIUS server.

Command Mode

Global Configuration mode

User Guidelines

The RADIUS server can place a port in a particular VLAN based on the result of the authentication. VLAN assignment must be configured on the external RADIUS server.

Example

The following example enables RADIUS-assigned VLANs.

```
console(config)#aaa authorization network default
radius
```

enable authentication

Use the **enable authentication** command in Line Configuration mode to specify the authentication method list when accessing a higher privilege level from a remote telnet or console. To return to the default specified by the **enable authentication** command, use the **no** form of this command.

Syntax

enable authentication {**default** | *list-name*}

no enable authentication

- **default** — Uses the default list created with the **aaa authentication enable** command.
- *list-name* — Uses the indicated list created with the **aaa authentication enable** command. (Range: 1-12 characters)

Default Configuration

Uses the default set with the command **aaa authentication enable**.

Command Mode

Line Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the default authentication method when accessing a higher privilege level console.

```
console(config)# line console
```

```
console(config-line)# enable authentication default
```

enable password

Use the **enable password** command in Global Configuration mode to set a local password to control access to the privileged EXEC mode. To remove the password requirement, use the **no** form of this command.

Syntax

enable password *password* [**encrypted**]

no enable password

- *password* — Password for this level (Range: 8- 64 characters).
- **encrypted** — Encrypted password entered, copied from another switch configuration.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines password "xxxyyyzzz" to control access to user and privilege levels.

```
console(config)# enable password xxxyyyzzz
```

ip http authentication

Use the **ip http authentication** command in Global Configuration mode to specify authentication methods for http server users. To return to the default, use the **no** form of this command.

Syntax

ip http authentication *method1* [*method2...*]

no ip http authentication

- method1* [*method2...*] — Specify at least one from the following table:

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is checked. This action has the same effect as the command **ip http authentication local**.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

Example

The following example configures the http authentication.

```
console(config)# ip http authentication radius local
```

ip https authentication

Use the **ip https authentication** command in Global Configuration mode to specify authentication methods for https server users. To return to the default configuration, use the **no** form of this command.

Syntax

ip https authentication *method1* [*method2...*]

no ip https authentication

- *method1* [*method2...*] — Specify at least one from the following table:

Keyword	Source or destination
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is checked. This action has the same effect as the command **ip https authentication local**.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. If **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

Example

The following example configures https authentication.

```
console(config)# ip https authentication radius local
```


login authentication

Use the **login authentication** command in Line Configuration mode to specify the login authentication method list for a line (console, telnet, or SSH). To return to the default specified by the authentication login command, use the **no** form of this command.

Syntax

login authentication {**default**|*list-name*}

no login authentication

- **default** — Uses the default list created with the **aaa authentication login** command.
- *list-name* — Uses the indicated list created with the **aaa authentication login** command.

Default Configuration

Uses the default set with the command **aaa authentication login**.

Command Mode

Line Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the default authentication method for a console.

```
console(config)# line console
console(config-line)# login authentication default
```

password (Line Configuration)

Use the **password** command in Line Configuration mode to specify a password on a line. To remove the password, use the **no** form of this command.

Syntax

password *password* [**encrypted**]

no password

- *password* — Password for this level. (Range: 8- 64 characters)
- **encrypted** — Encrypted password to be entered, copied from another switch configuration.

Default Configuration

No password is specified.

Command Mode

Line Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies a password "mcmxxyyy" on a line.

```
console(config-line)# password mcmxxyyy
```

password (User EXEC)

Use the **password** command in User EXEC mode to allow a user to change the password for only that user. This command should be used after the password has aged. The user is prompted to enter the old password and the new password.

Syntax

password

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows the prompt sequence for executing the password command.

```
console>password
Enter old password:*****
Enter new password:*****
Confirm new password:*****
```

show authentication methods

Use the **show authentication methods** command in Privileged EXEC mode to display information about the authentication methods.

Syntax

show authentication methods

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the authentication configuration.

```
console#show authentication methods
```

```
Login Authentication Method Lists
```

```
-----
```

```
defaultList          :  local
```

```
Enable Authentication Method Lists
```

```
-----
```

```
enableList           :  local
```

Line	Login Method List	Enable Method List
-----	-----	-----
Console	defaultList	enableList
Telnet	defaultList	enableList
SSH	defaultList	enableList
HTTPS	:local	
HTTP	:local	
DOT1X	:none	

show users accounts

Use the `show users accounts` command in Privileged EXEC mode to display information about the local user database.

Syntax

`show users accounts [long]`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the local user database.

```
console#show users accounts
```

UserName	Privilege	Password	Password	
Lockout				
		Aging	Expiry date	
-----	-----	-----	-----	-

admin	15	---	---	False
guest	1	---	---	False

show users login-history

Use the `show users login-history` command in Global Configuration mode to display information about the login history of users.

Syntax

`show users login-history [long]`

- *name* — name of user. (Range: 1-20 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example show user login history outputs.

```
console#show users login-history
```

Login Time	Username	Protocol	Location
Jan 19 2005 08:23:48	Bob	Serial	
Jan 19 2005 08:29:29	Robert	HTTP	172.16.0.8
Jan 19 2005 08:42:31	John	SSH	172.16.0.1
Jan 19 2005 08:49:52	Betty	Telnet	172.16.1.7

username

Use the **username** command in Global Configuration mode to add a new user to the local users database. To remove a user name use the **no** form of this command.

Syntax

username *name* **password** *password* [**level** *level*] [**encrypted**]

no username *name*

- *name* — The name of the user. (Range: 1-20 characters)
- *password* — The authentication password for the user. (Range: 8-64 characters. This value can be 0 [zero] if the no passwords min-length command has been executed.)
- *level* — The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. (Range: 0-15)
- **encrypted** — Encrypted password entered, copied from another switch configuration.

Default Configuration

No user name is defined.

The default privilege level is 1.

Command Mode

Global Configuration mode

User Guidelines

This command can be used to unlock a locked user account for an already existing user.

Example

The following example configures user "bob" with password "xxxxyyymmmmm" and user level 15.

```
console(config)# username bob password xxxxyyyymmmmm
level 15
```


ACL Commands

This chapter explains the following commands:

- access-list
- deny | permit
- ip access-group
- no ip access-group
- mac access-group
- mac access-list extended
- mac access-list extended rename
- show ip access-lists
- show mac access-list

access-list

Use the **access-list** command in Global Configuration mode to create an Access Control List (ACL) that is identified by the parameter *list-name*.

Syntax

```
access-list std-list-num {deny | permit} {srcip srcmask | every} [log]
[assign-queue queue-id] [redirect interface | mirror interface]
```

```
access-list ext-list-num {deny | permit} {every | {[icmp | igmp | ip | tcp |
udp | number] {srcip srcmask | any} [eq [portkey | portvalue]] {dstip
dstmask | any} [eq [portkey | portvalue]] [precedence precedence | tos tos
tosmask | dscp dscp] [log] [assign-queue queue-id] [redirect interface |
mirror interface]}}
```

no access-list *list-name*

- *list-name* — Access-list name up to 31 characters in length.
- **deny | permit** — Specifies whether the IP ACL rule permits or denies an action.
- **every** — Allows all protocols.
- **eq** — Equal. Refers to the Layer 4 port number being used as match criteria. The first reference is source match criteria, the second is destination match criteria.
- *number* — Standard protocol number. Protocol keywords icmp,igmp,ip,tcp,udp.
- *srcip* — Source IP address.
- *srcmask* — Source IP mask.
- *dstip* — Destination IP address.
- *dstmask* — Destination IP mask.
- *portvalue* — The source layer 4 port match condition for the ACL rule is specified by the port value parameter (Range: 0–65535).
- *portkey* — Or you can specify the *portkey*, which can be one of the following keywords: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www.
- **log** — Specifies that this rule is to be logged.

- **assign-queue** *queue-id*— Specifies the particular hardware queue for handling traffic that matches the rule. (Range: 0-6)
- **mirror** *interface*— Allows the traffic matching this rule to be copied to the specified interface.
- **redirect** *interface*— This parameter allows the traffic matching this rule to be forwarded to the specified unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Users are permitted to add rules, but if a packet does not match any user-specified rules, the packet is dropped by the implicit "deny all" rule.

Examples

The following examples create an ACL to discard any HTTP traffic from 192.168.77.171, but allow all other traffic from 192.168.77.171:

```
console(config)#access-list alpha deny 192.168.77.171
0.0.0.0 0.0.0.0 255.255.255.255 eq http

console(config)#access-list alpha permit
192.168.77.171 0.0.0.0
```

deny | permit

Use the **deny** command in Mac-Access-List Configuration mode to deny traffic if the conditions defined in the deny statement are matched. Use the **permit** command in Mac-Access-List Configuration mode to allow traffic if the conditions defined in the permit statement are matched.

Syntax

{deny | permit} **{srcmac srcmacmask | any}** **{dstmac dstmacmask | any | bpdud}** **[{ethertypekey | 0x0600-0xFFFF}]** **[vlan eq 0-4095]** **[cos 0-7]** **[secondary-vlan eq 0-4095]** **[secondary-cos 0-7]** **[log]** **[assign-queue queue-id]** **[{mirror | redirect} interface]**

- *srcmac* — Valid source MAC address in format xxxx.xxxx.xxxx.
- *srcmacmask* — Valid MAC address bitmask for the source MAC address in format xxxx.xxxx.xxxx.
- **any** — Packets sent to or received from any MAC address
- *dstmac* — Valid destination MAC address in format xxxx.xxxx.xxxx.
- *dstmacmask* — Valid MAC address bitmask for the destination MAC address in format xxxx.xxxx.xxxx.
- **bpdud** — Bridge protocol data unit
- *ethertypekey* — Either a keyword or valid four-digit hexadecimal number. (Range: Supported values are appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmlcast, mplsucast, Netbios, novell, pppoe, rarp.)
- *0x0600-0xFFFF* — Specify custom ethertype value (hexadecimal range 0x0600-0xFFFF)
- **vlan eq** — VLAN number. (Range 0-4095)
- **cos** — Class of service. (Range 0-7)
- **log** — Specifies that this rule is to be logged.
- **assign-queue** — Specifies particular hardware queue for handling traffic that matches the rule.
- *queue-id* — 0-6, where n is number of user configurable queues available for that hardware platform.
- **mirror** — Copies the traffic matching this rule to the specified interface.
- **redirect** — Forwards traffic matching this rule to the specified physical interface.
- *interface* — Valid physical interface in *unit/<port-type>port* format, for example l/g12.

Default Configuration

This command has no default configuration.

Command Mode

Mac-Access-List Configuration mode

User Guidelines

The **no** form of this command is not supported, as the rules within an ACL cannot be deleted individually. Rather the entire ACL must be deleted and respecified.

The assign-queue and redirect parameters are only valid for permit commands.

Example

The following example configures a MAC ACL to deny traffic from MAC address 0806.c200.0000.

```
console(config)#mac access-list extended DELL123
console(config-mac-access-list)#deny 0806.c200.0000
ffff.ffff.ffff any
```

ip access-group

no ip access-group

Use the **ip access-group** or **no ip access-group** command to apply/disable an IP based egress ACL on an Ethernet interface or a group of interfaces. An IP based ACL should have been created by the **access-list <name> ...** command with the same name specified in this command.

Syntax

ip access-group *name direction seqnum*

- *name* — Access list name. (Range: Valid IP access-list name up to 31 characters in length)
- *direction* — Direction of the ACL. (Range: In or out. Default is *in*.)

- *seqnum* — Precedence for this interface and direction. A lower sequence number has higher precedence. Range: 1 – 4294967295. Default is 1.

Default Configuration

This command has no default configuration.

Command Mode

Global and Interface Configuration

User Guidelines

Global mode command configures the ACL on all the interfaces, whereas the interface mode command does so for the interface.

Examples

```
console(config)#ip access-group aclname in
console(config)#no ip access-group aclname in
console(config)#ip access-group aclname1 out
console(config-if-1/g1)#ip access-group aclname out 2
console(config-if-1/g1)#no ip access-group aclname
out
```

mac access-group

Use the **mac access-group** command in Global Configuration or Interface Configuration mode to attach a specific MAC Access Control List (ACL) to an interface in a given direction.

Syntax

mac access-group *name sequence*

no mac access-group *name*

- *name* — Name of the existing MAC access list. (Range: 1-31 characters)
- *sequence* — Order of access list relative to other access lists already assigned to this interface and direction. (Range: 1-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode or Interface Configuration (Ethernet, VLAN or Port Channel) mode

User Guidelines

An optional sequence number may be specified to indicate the order of this access-list relative to the other access-lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number already is in use for this interface and direction, the specified access-list replaces the currently attached access list using that sequence number. If the sequence number is not specified for this command, a sequence number is selected that is one greater than the highest sequence number currently in use for this interface and direction.

This command specified in Interface Configuration mode only affects a single interface.

Example

The following example assigns a MAC access group to port 1/g1 with the name DELL123.

```
console(config)#interface 1/g1
console(config-if-1/g1)#mac access-group DELL123
```

mac access-list extended

Use the **mac access-list extended** command in Global Configuration mode to create the MAC Access Control List (ACL) identified by the *name* parameter.

Syntax

mac access-list extended *name*

no mac access-list extended *name*

- *name* — Name of the access list. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Use this command to create a mac access control list. The CLI mode is changed to Mac-Access-List Configuration when this command is successfully executed.

Example

The following example creates MAC ACL and enters MAC-Access-List-Configuration mode.

```
console(config)#mac access-list extended LVL7DELL
console(config-mac-access-list)#
```


mac access-list extended rename

Use the **mac access-list extended rename** command in Global Configuration mode to rename the existing MAC Access Control List (ACL).

Syntax

mac access-list extended rename *name newname*

- *name* — Existing name of the access list. (Range: 1-31 characters)
- *newname* — New name of the access list. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Command fails if the new name is the same as the old one.

Example

The following example shows the **mac access-list extended rename** command.

```
console(config)#mac access-list extended rename DELL1  
DELL2
```

show ip access-lists

Use the `show ip access-lists` command in Privileged EXEC mode to display access lists applied on interfaces and all rules that are defined for the access lists.

Syntax

`show ip access-lists accesslistname`

- *accesslistname* — The name used to identify the ACL. The range is 1-31 characters.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays IP ACLs configured on a device.

```
console#show ip access-lists
```

```
Current number of ACLs: 2   Maximum number of ACLs: 100
```

ACL Name Vlan(s)	Rules	Interface(s)

ACL40	1	
ACL41	1	

show mac access-list

Use the `show mac access-list` command in Privileged EXEC mode to display a MAC access list and all of the rules that are defined for the ACL.

Syntax

`show mac access-list name`

- *name* — Identifies a specific MAC access list to display.

Default Configuration

This command has no default configuration

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a MAC access list and all associated rules.

```
console#show mac access-list DELL123
```

The command output provides the following information:

Fields	Description
MAC ACL Name	The name of the MAC access list.
Rules	The number of user-configured rules defined for the MAC ACL. The implicit 'deny all' rule defined at the end of every MAC ACL is not included.
Interfaces	Displays the list of interfaces (unit/port) to which the MAC ACL is attached in a given direction.

Address Table Commands

This chapter explains the following commands:

- bridge address
- bridge aging-time
- bridge multicast address
- bridge multicast filtering
- bridge multicast forbidden address
- bridge multicast forbidden forward-unregistered
- bridge multicast forward-all
- bridge multicast forward-unregistered
- clear bridge
- port security
- port security max
- show bridge address-table
- show bridge address-table count
- show bridge address-table static
- show bridge multicast address-table
- show bridge multicast filtering
- show ports security
- show ports security addresses

bridge address

Use the **bridge address** command in Interface Configuration mode to add a static MAC-layer station source address to the bridge table. To delete the MAC address, use the **no** form of the **bridge address** command (using the **no** form of the command without specifying a MAC address deletes all static MAC addresses belonging to this VLAN).

Syntax

bridge address *mac-address* {**ethernet** *interface*|**port-channel** *port-channel-number*} [**permanent**]

no bridge address [*mac-address*]

- *mac-address* — A valid MAC address in the format xxxx.xxxx.xxxx.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.
- **permanent** — The address can be deleted only by using the **no bridge address** command.

Default Configuration

No static addresses are defined. The default mode for an added address is permanent.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example adds a permanent static MAC-layer station source address 3aa2.64b3.a245 to the bridge table.

```
console(config-if-vlan1)#bridge address  
3AA2.64B3.A245 ethernet 1/g8 permanent
```

bridge aging-time

Use the **bridge aging-time** command in Global Configuration mode to set the aging time of the address. To restore the default, use the **no** form of the **bridge aging-time** command.

Syntax

bridge aging-time *seconds*

no bridge aging-time

- *seconds* — Time is the number of seconds. (Range: 10–1000000 seconds)

Default Configuration

300 seconds

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

In this example the bridge aging time is set to 400.

```
console(config)#bridge aging-time 400
```

bridge multicast address

Use the **bridge multicast address** command in Interface Configuration mode to register MAC-layer Multicast addresses to the bridge table and to add ports to the group statically. To deregister the MAC address, use the **no** form of the **bridge multicast address** command.

Syntax

bridge multicast address {*mac-multicast-address*|*ip-multicast-address*}

bridge multicast address {*mac-multicast-address*|*ip-multicast-address*}
[**add**|**remove**] {**ethernet** *interface-list*|**port-channel** *port-channel-number-list*}

no bridge multicast address {*mac-multicast-address*|*ip-multicast-address*}

- **add** — Adds ports to the group. If no option is specified, this is the default option.
- **remove** — Removes ports from the group.
- *mac-multicast-address* — MAC multicast address in the format xxxx.xxxx.xxxx.
- *ip-multicast-address* — IP multicast address.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port-channels.

Default Configuration

No Multicast addresses are defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

If the command is executed without **add** or **remove**, the command registers only the group in the bridge database.

Static Multicast addresses can be defined only on static VLANs.

Examples

The following example registers the MAC address.

```
console(config)#interface vlan 8  
  
console(config-if-vlan8)#bridge multicast address  
0100.5e02.0203
```

The following example registers the MAC address and adds ports statically.


```
console(config)#interface vlan 8
console(config-if-vlan8)#bridge multicast address
0100.5e02.0203 add ethernet 1/g1-1/g9, 1/g2
```

bridge multicast filtering

Use the **bridge multicast filtering** command in Global Configuration mode to enable filtering of Multicast addresses. To disable filtering of Multicast addresses, use the **no** form of the **bridge multicast filtering** command.

Syntax

bridge multicast filtering

no bridge multicast filtering

Default Configuration

Disabled. All Multicast addresses are flooded to all ports of the relevant VLAN.

Command Mode

Global Configuration mode

User Guidelines

If switches exist on the VLAN, do not change the unregistered Multicast addresses' state to drop on the switch ports.

If switches exist on the VLAN and IGMP snooping is not enabled, use the **bridge multicast forward-all** command to enable forwarding all Multicast packets to the Multicast routers.

Example

In this example, bridge Multicast filtering is enabled.

```
console(config)#bridge multicast filtering
```

bridge multicast forbidden address

Use the **bridge multicast forbidden address** command in Interface Configuration mode to forbid adding a specific Multicast address to specific ports. To return to the system default, use the **no** form of this command. If routers exist on the VLAN, do not change the unregistered multicast addresses state to *drop* on the routers ports.

Syntax

bridge multicast forbidden address {*mac-multicast-address*|*ip-multicast-address*} {**add** | **remove**} {**ethernet** *interface-list*|**port-channel** *port-channel-number-list*}

no bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*}

- **add** — Adds ports to the group.
- **remove** — Removes ports from the group.
- *mac-multicast-address* — MAC Multicast address.
- *ip-multicast-address* — IP Multicast address.
- *interface-list* — Separate nonconsecutive valid Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive valid port-channels with a comma and no spaces; use a hyphen to designate a range of port-channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, ensure that the Multicast group is registered.

Examples

In this example the MAC address 01:00:5e:02:02:03 is forbidden on port 2/g9 within VLAN 8.

```
console(config)#interface vlan 8
console(config-if-vlan8)#bridge multicast address
01:00:5e:02:02:03
console(config-if-vlan8)#bridge multicast forbidden
address 01:00:5e:02:02:03 add ethernet 2/g9
```

bridge multicast forbidden forward-unregistered

Use the `bridge multicast forbidden forward-unregistered` command in Interface Configuration mode to forbid Forwarding-unregistered-multicast-addresses. Use the `no` form of this command to return to the default.

Syntax

```
bridge multicast forbidden forward-unregistered
no bridge multicast forbidden forward-unregistered
```

Default Configuration

The default for this command is *not forbidden*.

Command Mode

Interface configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example forbids forwarding unregistered multicast addresses on VLAN8.

```
console(config-if-vlan8)#bridge multicast forbidden
forward-unregistered
```

bridge multicast forward-all

Use the **bridge multicast forward-all** command in Interface Configuration mode to enable forwarding of all Multicast packets. To restore the default, use the **no** form of the **bridge multicast forward-all** command.

Syntax

bridge multicast forward-all

no bridge multicast forward-all

Default Configuration

Forward-unregistered

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

In this example all VLAN1 Multicast packets are forwarded.

```
console(config-if-vlan1)#bridge multicast forward-all
```

bridge multicast forward-unregistered

Use the **bridge multicast forward-unregistered** command in Interface Configuration mode to enable the forwarding of unregistered multicast addresses.

Syntax

bridge multicast forward-unregistered

Default Configuration

Forward-unregistered

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

If routers exist on the VLAN, do not change the unregistered multicast addresses state to *drop* on the routers ports.



NOTE: Do not use the **bridge multicast forbidden forward-unregistered** command with the **bridge multicast forward-unregistered** command on the same interface.

Example

The following example displays how to enable forwarding of unregistered multicast addresses.

```
console(config-if-vlan1)#bridge multicast forward-unregistered
```

clear bridge

Use the **clear bridge** command in Privileged EXEC mode to remove any learned entries from the forwarding database.

Syntax

clear bridge

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

In this example, the bridge tables are cleared.

```
console#clear bridge
```

port security

Use the **port security** command in Interface Configuration mode to disable the learning of new addresses on an interface. To enable new address learning, use the **no** form of the **port security** command.

Syntax

port security [**discard**] [**trap** *seconds*]

no port security

- **discard** — Discards frames with unlearned source addresses. This is the default if no option is indicated.
- **trap** *seconds* — Sends SNMP traps and defines the minimal amount of time in seconds between two consecutive traps. (Range: 1–1000000)

Default Configuration

Disabled—No port security

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

When port security is enabled on an interface, all dynamic entries learned up to that point are flushed, and new entries can be learned only to the limit set by the **port security max** command. The default limit is 100 dynamic MAC addresses.

Example

In this example, frame forwarding is enabled without learning, and with traps sent every 100 seconds on port g1.

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#port security forward trap
100
```

port security max

Use the **port security max** command in Interface Configuration mode to configure the maximum addresses that can be learned on the port while the port is in port security mode. To return to the system default, use the **no** form of this command.

Syntax

port security max *max-addr*

no port security max

- **max-addr** — The maximum number of addresses that can be learning on the port. (Range: 0-100)

Default Configuration

The default value for this command is 100.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows using this command in Ethernet Interface Configuration mode.

```
console(config-if-1/g3)# port security max 80
```

show bridge address-table

Use the `show bridge address-table` command in Privileged EXEC mode to display all entries in the bridge-forwarding database.

Syntax

`show bridge address-table [vlan vlan] [ethernet interface / port-channel port-channel-number]`

- *vlan* — Specific valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

In this example, all classes of entries in the bridge-forwarding database are displayed.

```
console#show bridge address-table
```

Aging time is 300 Sec

Vlan	Mac Address	Port	Type
-----	-----	-----	-----
1	0000.0001.0000	1/g1	Dynamic
1	0000.8420.5010	1/g1	Dynamic
1	0000.E26D.2C2A	1/g1	Dynamic
1	0000.E89A.596E	1/g1	Dynamic
1	0001.02F1.0B33	1/g1	Dynamic

show bridge address-table count

Use the `show bridge address-table count` command in Privileged EXEC mode to display the number of addresses present in the Forwarding Database.

Syntax

`show bridge address-table count [vlan vlan|ethernet interface-number|port-channel port-channel-number]`

- *vlan* — Specifies a valid VLAN, such as VLAN 1
- *interface* — Specifies a valid Ethernet port
- *port-channel-number* — Specifies a valid port-channel-number

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the addresses in the Forwarding Database:

```
console#show bridge address-table count
```

```
Capacity: 8192
```

```
Used: 109
```

```
Static addresses: 2
```

```
Secure addresses: 1
```

```
Dynamic addresses: 97
```

```
Internal addresses: 9
```

show bridge address-table static

Use the **show bridge address-table static** command in Privileged EXEC mode to display static entries in the bridge-forwarding database.

Syntax

show bridge address-table static [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *vlan* — Specific valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

In this example, all static entries in the bridge-forwarding database are displayed.

```
console#show bridge address-table static
```

Vlan	Mac Address	Port	Type
----	-----	-----	-----
1	0001.0001.0001	1/g1	Static

show bridge multicast address-table

Use the `show bridge multicast address-table` command in Privileged EXEC mode to display Multicast MAC address table information.

Syntax

`show bridge multicast address-table [vlan vlan-id] [address mac-multicast-address | ip-multicast-address] [format ip | mac]`

- *vlan_id* — A valid VLAN ID value.
- *mac-multicast-address* — A valid MAC Multicast address.
- *ip-multicast-address* — A valid IP Multicast address.
- *format* — Multicast address format. Can be *ip* or *mac*.

Default Configuration

If format is unspecified, the default is *mac*.

Command Mode

Privileged EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is in the range 01:00:5e:00:00:00 through 01:00:5e:7f:ff:ff.

Example

In this example, Multicast MAC address table information is displayed.

```
console#show bridge multicast address-table
```

Vlan	MAC Address	Type	Ports
-----	-----	-----	-----
1	0100.5E05.0505	Static	

Forbidden ports for multicast addresses:

Vlan	MAC Address	Ports
1	0100.5E05.0505	



NOTE: A multicast MAC address maps to multiple IP addresses, as shown above.

show bridge multicast filtering

Use the **show bridge multicast filtering** command in Privileged EXEC mode to display the Multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

- *vlan_id* — A valid VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

In this example, the Multicast configuration for VLAN 1 is displayed.

```
console#show bridge multicast filtering 1
```

```
Filtering: Disabled
```

```
VLAN: 1
```

```
Mode:
```

```
Forward-Unregistered
```

show ports security

Use the `show ports security` command in Privileged EXEC mode to display the port-lock status.

Syntax

`show ports security [ethernet interface | port-channel port-channel-number]`

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

In this example, all classes of entries in the port-lock status are displayed.

```
console#show ports security
```

Port	Status	Action	Maximum	Trap	Frequency
----	-----	-----	-----	-----	-----
1/g1	Locked	Discard	3	Enable	100
1/g2	Unlocked	-	28	-	-
1/g3	Locked	Discard, Shutdown	8	Disable	-

The following table describes the fields in this example.

Field	Description
Port	The port number.
Status	The status can be one of the following: Locked or Unlocked.
Actions	Action on violations.
Maximum	The maximum addresses that can be associated on this port in Static Learning mode or in Dynamic Learning mode.
Trap	Indicates if traps would be sent in case of violation.
Frequency	The minimum time between consecutive traps.

show ports security addresses

Use the `show ports security addresses` command in Privileged EXEC mode to display current dynamic addresses in locked ports.

Syntax

`show ports security addresses {ethernet interface|port-channel port-channel-number}`

- *interface* — Valid Ethernet port
- *port-channel-number* — Valid port-channel number

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays dynamic addresses for port channel number 1/g1.

```
console#show ports security addresses ethernet 1/g1
```

```
Dynamic addresses: 83
```

```
Maximum addresses: 100
```

```
Learned addresses
```

```
-----
```


CDP Interoperability Commands

This chapter explains the following commands:

- clear isdp counters
- clear isdp table
- isdp advertise-v2
- isdp enable
- isdp holdtime
- isdp timer
- show isdp
- show isdp entry
- show isdp interface
- show isdp neighbors
- show isdp traffic

clear isdp counters

The `clear isdp counters` command clears the ISDP counters.

Syntax

`clear isdp counters`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#clear isdp counters
```

clear isdp table

The `clear isdp table` command clears entries in the ISDP table.

Syntax

`clear isdp table`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#clear isdp table
```

isdp advertise-v2

The **isdp advertise-v2** command enables the sending of ISDP version 2 packets from the device. Use the “no” form of this command to disable sending ISDP version 2 packets.

Syntax

```
isdp advertise-v2
```

```
no isdp advertise-v2
```

Default Configuration

ISDP sends version 2 packets by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#isdp advertise-v2
```

isdp enable

The **isdp enable** command enables ISDP on the switch. Use the “no” form of this command to disable ISDP. Use this command in global configuration mode to enable the ISDP function on the switch. Use this command in interface mode to enable sending ISDP packets on a specific interface.

Syntax

```
isdp enable
```

```
no isdp enable
```

Default Configuration

ISDP is enabled.

Command Mode

Global Configuration mode.

Interface (Ethernet) configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example enables isdp on interface l/g1.

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#isdp enable
```

isdp holdtime

The **isdp holdtime** command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds. Use the “no” form of this command to reset the holdtime to the default.

Syntax

isdp holdtime *time*

no isdp holdtime

- *time* —The time in seconds (range 10–255 seconds).

Default Configuration

The default holdtime is 180 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets isdp holdtime to 40 seconds.

```
console(config)#isdp holdtime 40
```

isdp timer

The **isdp timer** command sets period of time between sending new ISDP packets. The range is given in seconds. Use the “no” form of this command to reset the timer to the default.

Syntax

isdp timer *time*

no isdp timer

- *time*—The time in seconds (range: 5–254 seconds).

Default Configuration

The default timer is 30 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the isdp timer value to 40 seconds.

```
console(config)#isdp timer 40
```

show isdp

The `show isdp` command displays global ISDP settings.

Syntax

`show isdp`

- `hostname`—The application will check to see if the Hostname configured on the switch is different from the default. If true, it uses the Hostname as the device ID. Otherwise, it uses the serial number as the device ID.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show isdp
Timer..... 30
Hold Time..... 180
Version 2 Advertisements..... Enabled
Neighbors table last time changed.... 0 days 00:06:01
Device ID..... QTFMPW82400020
Device ID format capability..... Serial Number
Device ID format..... Serial Number
```

```
(Switching) #hostname Dell-PC6248
(Dell-PC6248) #show isdp
Timer..... 30
Hold Time..... 180
Version 2 Advertisements..... Enabled
Neighbors table last time changed. 0 days 00:12:46
Device ID..... Dell-PC6248
Device ID format capability..... hostname
Device ID format..... hostname
```

show isdp entry

The `show isdp entry` command displays ISDP entries. If a device id specified, then only the entry about that device is displayed.

Syntax

`show isdp entry {all | deviceid}`

- **all** — Show ISDP settings for all devices.
- *deviceid* —The device ID associated with a neighbor.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show isdp entry Switch
```

Device ID	Switch
Address(es):	
IP Address:	172.20.1.18
IP Address:	172.20.1.18
Capability	Router IGMP
Platform	cisco WS-C4948
Interface	1/g1
Port ID	GigabitEthernet1/1
Holdtime	64
Advertisement Version	2
Entry last changed time	0 days 00:13:50
Version :	
Cisco IOS Software, Catalyst 4000 L3 Switch Software (cat4000 I9K91S-M), Version 12.2(25)EWA9, RELEASE SOFTWARE (fc3)	
Technical Support: http://www.cisco.com/techsupport	
Copyright (c) 1986-2007 by Cisco Systems, Inc.	
Compiled Wed 21-Mar-07 12:20 by tinhuang	

show isdp interface

The `show isdp interface` command displays ISDP settings for the specified interface.

Syntax

`show isdp interface {all | ethernet interface}`

- `all`—Show ISDP settings for all interfaces.
- `interface`—Specifies a valid interface. The full syntax is unit/port.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show isdp interface all
```

Interface	Mode
-----	-----
1/g1	Enabled
1/g2	Enabled
1/g3	Enabled
1/g4	Enabled
1/g5	Enabled
1/g6	Enabled
1/g7	Enabled

1/g8	Enabled
1/g9	Enabled
1/g10	Enabled
1/g11	Enabled
1/g12	Enabled
1/g13	Enabled
1/g14	Enabled
1/g15	Enabled
1/g16	Enabled
1/g17	Enabled
1/g18	Enabled
1/g19	Enabled
1/g20	Enabled
1/g21	Enabled
1/g22	Enabled
1/g23	Enabled
1/g24	Enabled

```
console#show isdp interface ethernet 1/g1
```

Interface	Mode
-----	-----
1/g1	Enabled

show isdp neighbors

The `show isdp neighbors` command displays the list of neighboring devices.

Syntax

`show isdp neighbors {ethernet interface | detail}`

- *interface* — Specifies a valid interface. The full syntax is unit/port.
- *detail* — Show detailed information about the neighbors.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show isdp neighbors
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route,

S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Intf	Hold	Cap.	Platform	Port
ID					

Switch	1/g1	165	RI	cisco WS-C4948	
GigabitEthernet1/1					

```
console#show isdp neighbors detail
```

```
Device ID                               Switch
Address(es) :
    IP Address:                         172.20.1.18
    IP Address:                         172.20.1.18
Capability                             Router IGMP
Platform                             cisco WS-C4948
Interface                             1/g1
Port ID                               GigabitEthernet1/1
Holdtime                              162
Advertisement Version                  2
Entry last changed time                0 days 00:55:20
Version :
Cisco IOS Software, Catalyst 4000 L3 Switch Software
(cat4000-I9K91S-M), Version 12.2(25)EWA9, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 21-Mar-07 12:20 by tinhuang
```

show isdp traffic

The show isdp traffic command displays ISDP statistics.

Syntax

```
show isdp traffic
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show isdp traffic
```

```
ISDP Packets Received..... 4253
ISDP Packets Transmitted..... 127
ISDPv1 Packets Received..... 0
ISDPv1 Packets Transmitted..... 0
ISDPv2 Packets Received..... 4253
ISDPv2 Packets Transmitted..... 4351
ISDP Bad Header..... 0
ISDP Checksum Error..... 0
ISDP Transmission Failure..... 0
ISDP Invalid Format..... 0

ISDP Table Full..... 392
ISDP Ip Address Table Full..... 737
```


DHCP Layer 2 Relay Commands

This chapter explains the following commands:

- `dhcp l2relay` (Global Configuration) (Global Configuration)
- `dhcp l2relay` (Interface Configuration) (Interface Configuration)
- `dhcp l2relay circuit-id`
- `dhcp l2relay remote-id`
- `dhcp l2relay trust`
- `dhcp l2relay vlan`

dhcp l2relay (Global Configuration)

Use the `dhcp l2relay` command to enable layer 2 DHCP relay functionality. The subsequent commands mentioned in this section can only be used when the L2-DHCP relay is enabled. Use the "no" form of this command to disable L2-DHCP relay.

Syntax

`dhcp l2relay`

`no dhcp l2relay`

Default Configuration

DHCP L2 Relay is disabled by default.

Command Mode

Global Configuration.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#dhcp l2relay
```

dhcp l2relay (Interface Configuration)

Use the `dhcp l2relay` command to enable DHCP L2 Relay for an interface. Use the "no" form of this command to disable DHCP L2 Relay for an interface.

Syntax

`dhcp l2relay`

`no dhcp l2relay`

Default Configuration

DHCP L2Relay is disabled on all interfaces by default.

Command Mode

Interface Configuration (Ethernet).

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-1/g1)#dhcp l2relay
```

dhcp l2relay circuit-id

Use the **dhcp l2relay circuit-id** command to enable setting the DHCP Option 82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82. Use the "no" form of this command to disable setting the DHCP Option 82 Circuit ID.

Syntax

```
dhcp l2relay circuit-id vlan vlan-range
```

```
no dhcp l2relay circuit-id vlan vlan-range
```

- *vlan-range* - The list of VLAN IDs.

Default Configuration

Setting the DHCP Option 82 Circuit ID is disabled by default.

Command Mode

Global Configuration

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#dhcp l2relay circuit-id vlan 340-350
```

dhcp l2relay remote-id

Use the `dhcp l2relay remote-id` command to enable setting the DHCP Option 82 Remote ID for a VLAN. When enabled, the supplied string is used for the Remote ID in DHCP Option 82. Use the "no" form of this command to disable setting the DHCP Option 82 Remote ID.

Syntax

`dhcp l2relay remote-id remoteId vlan vlan-range`

`no dhcp l2relay remote-id remoteId vlan vlan-range`

- *remoteId*—The string to be used as the remote ID in the Option 82 (Range: 1 - 128 characters).

Default Configuration

Setting the DHCP Option 82 Remote ID is disabled by default.

Command Mode

Global Configuration.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#dhcp l2relay remote-id dslforum vlan
10,20-30
```

dhcp l2relay trust

Use the **dhcp l2relay trust** command to configure an interface to mandate Option-82 on receiving DHCP packets.

Syntax

dhcp l2relay trust

no dhcp l2relay trust

Default Configuration

DHCP Option 82 is discarded by default.

Configuration Mode

Interface Configuration (Ethernet).

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-1/g1)#dhcp l2relay trust
```

dhcp l2relay vlan

Use the **dhcp l2relay vlan** command to enable the L2 DHCP Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing. Use the "no" form of this command to disable L2 DHCP Relay for a set of VLANs.

Syntax

dhcp l2relay vlan *vlan-range*

no dhcp l2relay vlan *vlan-range*

- *vlan-range* - The list of VLAN IDs.

Default Configuration

DHCP L2 Relay is disabled on all VLANs by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#dhcp l2relay vlan 10,340-345
```

DHCP Snooping Commands

This chapter explains the following commands:

- clear ip dhcp snooping statistics
- ip dhcp snooping
- ip dhcp snooping binding
- ip dhcp snooping database
- ip dhcp snooping database write-delay
- ip dhcp snooping limit
- ip dhcp snooping log-invalid
- ip dhcp snooping trust
- ip dhcp snooping verify mac-address
- show ip dhcp snooping
- show ip dhcp snooping binding
- show ip dhcp snooping database
- show ip dhcp snooping interfaces
- show ip dhcp snooping statistics

clear ip dhcp snooping statistics

Use the `clear ip dhcp snooping statistics` command to clear all DHCP Snooping statistics.

Syntax

`clear ip dhcp snooping statistics`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

```
console#clear ip dhcp snooping statistics
```

ip dhcp snooping

Use the `ip dhcp snooping` command to enable DHCP snooping globally or on a specific VLAN. Use the “no” form of this command to disable DHCP snooping.

Syntax

`ip dhcp snooping`

`no ip dhcp snooping`

Default Configuration

DHCP Snooping is disabled by default.

Command Mode

Global Configuration mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip dhcp snooping
```

```
console(config-if-vlan1,2,3)#ip dhcp snooping
```

ip dhcp snooping binding

Use the **ip dhcp snooping binding** command to configure a static DHCP Snooping binding. Use the “no” form of this command to remove a static binding.

Syntax

ip dhcp snooping binding *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface*

no ip dhcp snooping binding *mac-address*

- *mac-address*—The client's MAC address.
- *vlan-id*—The number of the VLAN the client is authorized to use.
- *ip-address*—The IP address of the client.
- *interface*—The interface on which the client is authorized. The form is unit/port.

Default Configuration

There are no static DHCP snooping bindings by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip dhcp snooping binding
00:00:00:00:00:01 vlan 10 10.131.12.134 interface
1/g1
```

ip dhcp snooping database

Use the **ip dhcp snooping database** command to configure the persistent storage location of the DHCP snooping database. This can be local to the switch or on a remote machine.

Syntax

ip dhcp snooping database {**local** | **tftp://hostIP/filename**}

- *hostIP*—The IP address of the remote host.
- *filename*—The name of the file for the database on the remote host.

Default Configuration

The database is stored locally by default.

Configuration Mode

Global Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the storage location of the snooping database as local.

```
console(config)#ip dhcp snooping database local
```


The following example configures the storage location of the snooping database as remote.

```
console(config)#ip dhcp snooping database  
tftp://10.131.11.1/db.txt
```

ip dhcp snooping database write-delay

Use the **ip dhcp snooping database write-delay** command to configure the interval in seconds at which the DHCP Snooping database will be stored in persistent storage. Use the “no” form of this command to reset the write delay to the default.

Syntax

ip dhcp snooping database write-delay *seconds*

no ip dhcp snooping database write-delay

- *seconds*—The write delay (Range: 15–86400 seconds).

Default Configuration

The write delay is 300 seconds by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip dhcp snooping database write-delay  
500
```

ip dhcp snooping limit

Use the **ip dhcp snooping limit** command to control the maximum rate of DHCP messages. Use the “no” form of this command to reset the limit to the default.

Syntax

ip dhcp snooping limit {none | rate *pps* [burst interval *seconds*]}

no ip dhcp snooping limit

- *pps*—The maximum number of packets per second allowed (Range: 0–300 pps).
- *seconds*—The time allowed for a burst (Range: 1–15 seconds).

Default Configuration

The default maximum rate is 15 packets per second (pps).

The default burst interval is 1 second.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Examples

```
console(config-if-1/g1)#ip dhcp snooping limit none
```

```
console(config-if-1/g1)#ip dhcp snooping limit rate  
100 burst interval 1
```

ip dhcp snooping log-invalid

Use the `ip dhcp snooping log-invalid` command to enable logging of DHCP messages filtered by the DHCP Snooping application. Use the “no” form of this command to disable logging.

Syntax

`ip dhcp snooping log-invalid`

`no ip dhcp snooping log-invalid`

Default Configuration

Logging of filtered messages is disabled by default.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-1/g1)#ip dhcp snooping log-invalid
```

```
console(config-if-1/g1)#no ip dhcp snooping log-  
invalid
```

ip dhcp snooping trust

Use the `ip dhcp snooping trust` command to configure a port as trusted. Use the “no” form of this command to configure a port as untrusted.

Syntax

`ip dhcp snooping trust`

`no ip dhcp snooping trust`

Default Configuration

Ports are untrusted by default.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-1/g1)#ip dhcp snooping trust
```

```
console(config-if-1/g1)#no ip dhcp snooping trust
```

ip dhcp snooping verify mac-address

Use the **ip dhcp snooping verify mac-address** command to enable the verification of the source MAC address with the client MAC address in the received DHCP message. Use the “no” form of this command to disable verification of the source MAC address.

Syntax

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Default Configuration

Source MAC address verification is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip dhcp snooping verify mac-address
```

show ip dhcp snooping

Use the **show ip dhcp snooping** command to display the DHCP snooping global and per port configuration.

Syntax

```
show ip dhcp snooping
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip dhcp snooping
```

```
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40
```

Interface	Trusted	Log Invalid Pkts
-----	-----	-----
1/g1	Yes	No

1/g2	No	Yes
1/g3	No	Yes
1/g4	No	No
1/g6	No	No

show ip dhcp snooping binding

Use the `show ip dhcp snooping binding` command to display the DHCP snooping binding entries.

Syntax

`show ip dhcp snooping binding [{static | dynamic}] [interface port] [vlan vlan-id]`

- **static | dynamic**—Use these keywords to filter by static or dynamic bindings.
- *port*—The interface for which to show bindings. Format is unit/port.
- *vlan-id*—The number of the VLAN for which to show bindings.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip dhcp snooping binding
```

```
Total number of bindings: 2
```

MAC Address	IP Address	VLAN	Interface	Lease time (Secs)
-----	-----	----	-----	-----
00:02:B3:06:60:80	210.1.1.3	10	1/g1	86400
00:0F:FE:00:13:04	210.1.1.4	10	1/g1	86400

show ip dhcp snooping database

Use the `show ip dhcp snooping database` command to display the DHCP snooping configuration related to the database persistence.

Syntax

`show ip dhcp snooping database`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip dhcp snooping database
```

```
agent url: /10.131.13.79:/sail.txt
```

```
write-delay: 5000
```

show ip dhcp snooping interfaces

Use the `show ip dhcp snooping interfaces` command to show the DHCP Snooping status of the interfaces.

Syntax

`show ip dhcp snooping interfaces interface`

- `interface`—A valid physical interface.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip dhcp snooping interfaces
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
-----	-----	-----	-----
1/g1	No	15	1
1/g2	No	15	1
1/g3	No	15	1


```
console#show ip dhcp snooping interfaces ethernet
1/g15
```

Interface	Trust State	Rate Limit (pps)	Burst Interval (seconds)
-----	-----	-----	-----
1/g15	Yes	15	1

show ip dhcp snooping statistics

Use the show ip dhcp snooping statistics command to display the DHCP snooping filtration statistics.

Syntax

```
show ip dhcp snooping statistics
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

The following fields are displayed by this command:

MAC Verify Failures	The number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client MAC address mismatch.
Client Ifc Mismatch	The number of DHCP release and Deny messages received on the different ports than previously learned.
DHCP Server Msgs	The number of DHCP server messages received on untrusted ports.

Example

console#show ip dhcp snooping statistics

Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs Rec'd
-----	-----	-----	-----
1/g2	0	0	0
1/g3	0	0	0
1/g4	0	0	0
1/g5	0	0	0
1/g6	0	0	0
1/g7	0	0	0
1/g8	0	0	0
1/g9	0	0	0
1/g10	0	0	0
1/g11	0	0	0
1/g12	0	0	0
1/g13	0	0	0
1/g14	0	0	0
1/g15	0	0	0
1/g16	0	0	0
1/g17	0	0	0
1/g18	0	0	0
1/g19	0	0	0
1/g20	0	0	0

Dynamic ARP Inspection Commands

This chapter explains the following commands:

- arp access-list
- clear counters ip arp inspection
- ip arp inspection filter
- ip arp inspection limit
- ip arp inspection trust
- ip arp inspection validate
- ip arp inspection vlan
- permit ip host mac host
- show arp access-list
- show ip arp inspection ethernet
- show ip arp inspection statistics
- show ip arp inspection vlan

arp access-list

Use the **arp access-list** command to create an ARP ACL. It will place the user in ARP ACL Configuration mode. Use the “no” form of this command to delete an ARP ACL.

Syntax

arp access-list *acl-name*

no arp access-list *acl-name*

- *acl-name* — A valid ARP ACL name (Range: 1–31 characters).

Default Configuration

There are no ARP ACLs created by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#arp access-list tier1
```

clear counters ip arp inspection

Use the **clear counters ip arp inspection** command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Syntax

clear counters ip arp inspection

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#clear counters ip arp inspection
```

ip arp inspection filter

Use the **ip arp inspection filter** command to configure the ARP ACL to be used for a single VLAN or a range of VLANs to filter invalid ARP packets. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings. Use the “no” form of this command to unconfigure the ARP ACL.

Syntax

ip arp inspection filter *acl-name* **vlan** *vlan-range* [**static**]

no ip arp inspection filter *acl-name* **vlan** *vlan-range* [**static**]

- *acl-name* —The name of a valid ARP ACL. (Range: 1–31 characters)
- *vlan-range* —A valid VLAN range.

Default Configuration

No ARP ACL is configured.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip arp inspection filter tier1 vlan 2-10 static
```

```
console(config)#ip arp inspection filter tier1 vlan 20-30
```

ip arp inspection limit

Use the **ip arp inspection limit** command to configure the rate limit and burst interval values for an interface.

Configuring ‘none’ for the limit means the interface is not rate limited for Dynamic ARP Inspection.



NOTE: The maximum pps value shown in the range for the rate option might be more than the hardware allowable limit. The user needs to understand the box performance and configure the maximum rate pps accordingly.

Syntax

```
ip arp inspection limit {none | rate pps [burst interval seconds]}
```

```
no ip arp inspection limit
```

- **none** — To set no rate limit.
- *pps* — The number of packets per second (Range: 0–300).
- *seconds* — The number of seconds (Range: 1–15).

Default Configuration

The default rate limit is 15 packets per second.

The default burst interval is 1 second.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-1/g1)#ip arp inspection limit none
console(config-if-1/g1)#ip arp inspection limit rate
100 burst interval 2
```

ip arp inspection trust

The `ip arp inspection trust` command configures an interface as trusted for Dynamic ARP Inspection. Use the “no” form of this command to configure an interface as untrusted.

Syntax

```
ip arp inspection trust
no ip arp inspection trust
```

Default Configuration

Interfaces are configured as untrusted by default.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-1/g3)#ip arp inspection trust
```

ip arp inspection validate

Use the **ip arp inspection validate** command to enable additional validation checks like source MAC address validation, destination MAC address validation or IP address validation on the received ARP packets. Each command overrides the configuration of the previous command. For example, if a command enables source MAC address and destination MAC address validations and a second command enables IP address validation only, the source MAC address and destination MAC address validations are disabled as a result of the second command. Use the “no” form of this command to disable additional validation checks.

Syntax

ip arp inspection validate {[src-mac] [dst-mac] [ip]}

no ip arp inspection validate {[src-mac] [dst-mac] [ip]}

- **src-mac**—For validating the source MAC address of an ARP packet.
- **dst-mac**—For validating the destination MAC address of an ARP packet.
- **ip**—For validating the IP address of an ARP packet.

Default Configuration

There is no additional validation enabled by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command

Example

```
console(config)#ip arp inspection validate src-mac  
dst-mac ip
```

```
console(config)#ip arp inspection validate src-mac ip
```

```
console(config)#ip arp inspection validate dst-mac ip
```

```
console(config)#ip arp inspection validate ip
```


ip arp inspection vlan

Use the **ip arp inspection vlan** command to enable Dynamic ARP Inspection on a single VLAN or a range of VLANs. Use the “no” form of this command to disable Dynamic ARP Inspection on a single VLAN or a range of VLANs.

Syntax

ip arp inspection vlan *vlan-range* [**logging**]

no ip arp inspection vlan *vlan-range* [**logging**]

- *vlan-range* — A valid range of VLAN IDs.
- **logging** — Use this parameter to enable logging of invalid packets.

Default Configuration

Dynamic ARP Inspection is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip arp inspection vlan 200-300
console(config)#ip arp inspection vlan 200-300
logging
```

permit ip host mac host

Use the **permit ip host mac host** command to configure a rule for a valid IP address and MAC address combination used in ARP packet validation. Use the “no” form of this command to delete an ARP ACL rule.

Syntax

permit ip host *sender-ip* **max host** *sender-mac*

no permit ip host *sender-ip* **max host** *sender-mac*

- *sender-ip* — Valid IP address used by a host.
- *sender-mac* — Valid MAC address in combination with the above sender-ip used by a host.

Default Configuration

There are no ARP ACL rules created by default.

Command Mode

ARP Access-list Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(Config-arp-access-list)#permit ip host  
1.1.1.1 mac host 00:01:02:03:04:05
```

show arp access-list

Use the **show arp access-list** command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument would display only the rules in that ARP ACL.

Syntax

show arp access-list [*acl-name*]

acl-name — A valid ARP ACL name (Range: 1–31 characters).

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

```
console#show arp access-list
ARP access list H2
    permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
    permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
ARP access list H3
ARP access list H4
    permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
```

show ip arp inspection ethernet

Use the **show ip arp inspection ethernet** command to display the Dynamic ARP Inspection configuration on all the DAI enabled interfaces. Giving an interface argument, it displays the values for that interface.

Syntax

show ip arp inspection ethernet [*interface*]

- *interface* — Valid Ethernet port. The full syntax is unit/port.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

The following fields are displayed for each interface:

Interface	The interface-id for each displayed row.
Trust State	Whether interface is trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds.

Example

```
console#show ip arp inspection ethernet
```

Interface	Trust State	Rate Limit	Burst
Interval		(pps)	(seconds)
-----	-----	-----	-----
1/g1	Untrusted	15	
1			
1/g2	Untrusted	10	
10			

show ip arp inspection statistics

Use the `show ip arp inspection statistics` command to display the statistics of the ARP packets processed by Dynamic ARP Inspection. Given `vlan-range` argument, it displays the statistics on all DAI enabled Vlan's in that range. In the case of no argument, it lists the summary of the forwarded and dropped ARP packets.

Syntax

`show ip arp inspection statistics [vlan vlan-range]`

- *vlan-range* —A valid VLAN range.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The following information is displayed for each VLAN when a VLAN range is supplied:

VLAN	The Vlan-Id for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this Vlan.
Dropped	The total number of invalid ARP packets dropped in this Vlan.
DHCP Drops	The number of packets dropped due to DHCP Snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.

Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

Example

console#show ip arp inspection statistics

VLAN	Forwarded	Dropped
----	-----	-----
10	90	14
20	10	3

console#show ip arp inspection statistics vlan 10,20

VLAN	DHCP	ACL	DHCP	ACL	Bad
Src	Bad Dest	Invalid			
	Drops	Drops	Permits	Permits	MAC
MAC	IP				
-----	-----	-----	-----	-----	-----
10	11	1	65	25	
1	1	0			
20	1	0	8	2	
0	1	1			

show ip arp inspection vlan

Use the **show ip arp inspection vlan** command to display the Dynamic ARP Inspection configuration on all the VLANs in the given VLAN range. It also displays the global configuration values for source MAC validation, destination MAC validation and invalid IP validation.

Syntax

show ip arp inspection vlan [*vlan-range*]

vlan-range — A valid VLAN range.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The following global parameters are displayed:

Source Mac Validation	If Source Mac validation of ARP frame is enabled.
Destination Mac Validation	If Destination Mac validation of ARP Response frame is enabled.
IP Address Validation	If IP address validation of ARP frame is enabled.

The following fields are displayed for each VLAN:

Vlan	The Vlan-Id for each displayed row.
Configuration	Whether DAI is enabled on the Vlan.
Log Invalid	Whether logging of invalid ARP packets is enabled on the Vlan.
ACL Name	ARP ACL Name if configured on the Vlan
Static flag	If the ARP ACL is configured static on the Vlan

Example

console#show ip arp inspection vlan 10-12

Source Mac Validation : Disabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled

Vlan Static flag	Configuration	Log Invalid	ACL Name
----	-----	-----	-----
-- -----			
10 Enabled	Enabled	Enabled	H2
11	Disabled	Enabled	
12	Enabled	Disabled	

Ethernet Configuration Commands

This chapter explains the following commands:

- clear counters
- description
- duplex
- flowcontrol
- interface ethernet
- interface range ethernet
- mtu
- negotiation
- show interfaces advertise
- show interfaces configuration
- show interfaces counters
- show interfaces description
- show interfaces detail
- show interfaces status
- show statistics ethernet
- show storm-control
- shutdown
- speed
- storm-control broadcast
- storm-control multicast
- storm-control unicast

clear counters

Use the **clear counters** command in Privileged EXEC mode to clear statistics on an interface.

Syntax

clear counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface* — Valid Ethernet port. The full syntax is: *unit/port*
- *port-channel-number* — Valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

In the following example, the counters for port 1/g1 are cleared.

```
console#clear counters ethernet 1/g1
```

description

Use the **description** command in Interface Configuration mode to add a description to an interface. To remove the description use the **no** form of this command.

Syntax

description *string*

no description

- *string* — Comment or a description of the port attached to this interface. (Range: 1 to 64 characters)

Default Configuration

By default, the interface does not have a description.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example adds a description to the Ethernet port 5.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)# description RD_SW#3
```

duplex

Use the **duplex** command in Interface Configuration mode to configure the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. To restore the default, use the **no** form of this command.

Syntax

duplex {half | full}

no duplex

- **half** — Force half-duplex operation
- **full** — Force full-duplex operation

Default Configuration

The interface is set to full duplex.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the duplex operation of Ethernet port 5 to force full duplex operation.

```
console(config)# interface ethernet 1/g5
console(config-if-1/g5)# duplex full
```

flowcontrol

Use the **flowcontrol** command in Global Configuration mode to configure the flow control. To disable flow control, use the **no** form of this command.

Syntax

flowcontrol

no flowcontrol

Default Configuration

Flow Control is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

In the following example, flow control is enabled.

```
console(config)# flowcontrol
```

interface ethernet

Use the **interface ethernet** command in Global Configuration mode to enter the interface configuration mode to configure an Ethernet type interface.

Syntax

interface ethernet *interface*

- *interface* — Valid Ethernet port. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables port 5/g18 for configuration.

```
console(config)# interface ethernet 5/g18
```

interface range ethernet

Use the **interface range ethernet** command in Global Configuration mode to execute a command on multiple ports at the same time.

Syntax

interface range ethernet {*port-range* / all}

- *port-range* — List of valid ports to configure. Separate non consecutive ports with a comma and no spaces; use a hyphen to designate a range of ports. For more detailed information, refer to the Operating on Multiple Objects (Range) discussion in the Using the CLI chapter.
- **all** — All Ethernet ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each active interface in the range. If the command returns an error on one of the active interfaces, it does not stop executing commands on other active interfaces.

Example

The following example shows how ports 5/g18 to 5/g20 and ports 3/g1 to g24 are grouped to receive the same command.

```
console(config)# interface range ethernet 5/g18-  
5/g20,3/g1-3/g24  
  
console(config-if)#
```

mtu

Use the **mtu** command in Interface Configuration mode to enable jumbo frames on an interface by adjusting the maximum size of a packet. To return to the default setting, use the **no** form of this command.

Syntax

mtu *bytes*

no mtu

- *bytes* — Number of bytes (Range: 1518-9216)

Default Configuration

The default number of bytes is 1518 (1522 bytes of VLAN-tagged frames).

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The value set allows an additional four bytes for the VLAN tag.

Example

The following example of the `mtu` command increases maximum packet size to 9216 bytes.

```
console(config-if-1/g5) #mtu 9216
```

negotiation

Use the **negotiation** command in Interface Configuration mode to enable auto-negotiation operation for the speed and duplex parameters of a given interface. To disable negotiation, use the **no** form of this command.

Syntax

negotiation [**capability1** [**capability2**...**capability5**]]

no negotiation

- **capabilities** — Specifies capabilities to advertise. (Possible values: 10h, 10f, 100h, 100f, and 1000f)

Default Configuration

If unspecified, defaults to list of all capabilities of the port.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Entering the command `negotiation` with no parameters enables all capabilities. Note that if you have previously entered `negotiation` with capabilities, this action overwrites the previous configuration so that all capabilities are enabled.

Example

The following example enables auto negotiations on gigabit Ethernet port 5 of unit 1.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)#negotiation
```

show interfaces advertise

Use the **show interfaces advertise** command in Privileged EXEC mode to display information about auto-negotiation advertisement.

Syntax

```
show interfaces advertise [ethernet interface]
    • interface — A valid Ethernet port.
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display information about auto negotiation advertisement.

```
console#show interfaces advertise

Port   Type           Neg      Operational Link Advertisement
----   -
1/g2   1G-Copper      Enable   1000f, 100f, 100h, 10f, 10h
1/g2   1G-Copper      Enable   1000f
```



```

console# show interfaces advertise ethernet 1/g1
Port: Ethernet 1/g1
Type: 1G-Copper
Link state: Up
Auto negotiation: enabled
10h 10f 100h 100f 1000f
Admin Local Link -----
Advertisement yes      yes      yes      yes      no

```

show interfaces configuration

Use the **show interfaces configuration** command in User EXEC mode to display the configuration for all configured interfaces.

Syntax

show interfaces configuration [*ethernet interface* | *port-channel port-channel-number*]

- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no use guidelines.

Example

The following example displays the configuration for all configured interfaces:

```
console>show interfaces configuration
```

Port	Type	Duplex	Speed	Neg	Admin State
-----	-----	-----	-----	----	-----
1/g1	Gigabit - Level	Full	100	Auto	Up
1/g2	Gigabit - Level	N/A	Unknown	Auto	Up
1/g3	Gigabit - Level	N/A	Unknown	Auto	Up
1/g4	Gigabit - Level	N/A	Unknown	Auto	Up
1/g5	Gigabit - Level	N/A	Unknown	Auto	Up
1/g6	Gigabit - Level	N/A	Unknown	Auto	Up
1/g7	Gigabit - Level	N/A	Unknown	Auto	Up
1/g8	Gigabit - Level	N/A	Unknown	Auto	Up
1/g9	Gigabit - Level	N/A	Unknown	Auto	Up
1/g10	Gigabit - Level	N/A	Unknown	Auto	Up
1/g11	Gigabit - Level	N/A	Unknown	Auto	Up
1/g12	Gigabit - Level	N/A	Unknown	Auto	Up
1/g13	Gigabit - Level	N/A	Unknown	Auto	Up
1/g14	Gigabit - Level	N/A	Unknown	Auto	Up
1/g15	Gigabit - Level	N/A	Unknown	Auto	Up
1/g16	Gigabit - Level	N/A	Unknown	Auto	Up
1/g17	Gigabit - Level	N/A	Unknown	Auto	Up
1/g18	Gigabit - Level	N/A	Unknown	Auto	Up
1/g19	Gigabit - Level	N/A	Unknown	Auto	Up
--More-- or (q)uit					

The displayed port configuration information includes the following:

Field	Description
Port	The port number.
Port Type	The port designated IEEE shorthand identifier. For example 1000Base-T refers to 1000 Mbps baseband signaling including both Tx and Rx transmissions.
Duplex	Displays the port Duplex status.
Speed	Refers to the port speed.
Neg	Describes the Auto-negotiation status.
Admin State	Displays whether the port is enabled or disabled.

show interfaces counters

Use the **show interfaces counters** command in User EXEC mode to display traffic seen by the interface.

Syntax

show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays traffic seen by the physical interface:

```
console>show interfaces counters
```

Port	InOctets	InUcastPkts
------	----------	-------------

----	-----	-----
------	-------	-------

1/g1	183892	1289
------	--------	------

3/g1	123899	1788
------	--------	------

Port	OutOctets	OutUcastPkts
------	-----------	--------------

----	-----	-----
------	-------	-------

1/g1	9188	9
------	------	---

2/g1	0	0
------	---	---

3/g1	8789	27
------	------	----

Ch	InOctets	InUcastPkts
----	----------	-------------

----	-----	-----
------	-------	-------

1	27889	928
---	-------	-----

Ch	OutOctets	OutUcastPkts
----	-----------	--------------

----	-----	-----
------	-------	-------

1	23739	882
---	-------	-----

The following example displays counters for Ethernet port 1/g1.

```
console#show interfaces counters ethernet 1/g1
```

Port	InOctets	InUcastPkts
------	----------	-------------

----	-----	-----
------	-------	-------

1/g1	183892	1289
------	--------	------

```

Port   OutOctets      OutUcastPkts
----   -
1/g1   9188           9

```

```

Alignment Errors: 17
FCS Errors: 8
Single Collision Frames: 0
Multiple Collision Frames: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0

```

The following table describes the fields shown in the display:

Field	Description
InOctets	Counted received octets.
InUcastPkts	Counted received Unicast packets.
InMcastPkts	Counted received Multicast packets.
InBcastPkts	Counted received Broadcast packets.
OutOctets	Counted transmitted octets.
OutUcastPkts	Counted transmitted Unicast packets.
OutMcastPkts	Counted transmitted Multicast packets.
OutBcastPkts	Counted transmitted Broadcast packets.

Field	Description
Alignment Errors	A count of frames received that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	Counted frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Counted frames that are involved in a single collision, and are subsequently transmitted successfully.
Multiple Collision Frames	A count of frames that are involved in a multiple collision, and are subsequently transmitted successfully
Deferred Transmissions	A count of frames for which the first transmission attempt is delayed because the medium is busy
Late Collisions	Counted times that a collision is detected later than one slot time into the transmission of a packet.
Excessive Collisions	Counted frames for which transmission fails due to excessive collisions.
Oversize Packets	Counted frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	A count of frames for which reception fails due to an internal MAC sublayer receive error.
Received Pause Frames	A count of MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

show interfaces description

Use the **show interfaces description** command in User EXEC mode to display the description for all configured interfaces.

Syntax

show interfaces description [*ethernet interface* | *port-channel port-channel-number*]

- *interface* — Valid Ethernet port.
- *port-channel-number* — A valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the description for the interface 1/g1.

```
console>show interfaces description
```

```
Port Description
```

```
-----  
1/g1 Port that should be used for management only  
2/g1  
2/g2
```

```
Ch      Description  
-----  
1       Output
```

show interfaces detail

Add support for a single command that shows VLAN info, STP info, Port status info, Port configuration info. Add a command which wraps all the port commands into a single command.

Syntax

```
show interfaces detail [ethernet interface | port-channel port-channel-port-channel-number]
```

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel trunk index.

Default Configuration

There is no default configuration for this command.

Command Mode

User EXEC mode

User Guidelines

The command will be show interfaces detail {ethernet interface | port-channel port-channel-number} where

- *interface*—A valid Ethernet port.

port-channel-number—A valid port-channel trunk index.

This command will combine the output of the following commands:

- *show interfaces configuration* [*ethernet* interface | *port-channel* port-channel-number]
- *show interfaces description* [*ethernet* interface | *port-channel* port-channel-number]
- *show interfaces status* [*ethernet* interface | *port-channel* port-channel-number]
- *show interfaces switchport* {*ethernet* interface | *port-channel* port-channel-number}
- *show spanning-tree* [*ethernet* interface-number | *port-channel* port-channel-number] [instance instance-id]

Example

```
console#show interfaces detail Ethernet 1/xg1
```

Port	Type	Duplex	Speed	Neg	Admin State	Link State
1/xg1	10G	N/A	Unknown	Auto	Down	Inactive

Port Description

1/xg1 ExampleName

VLAN Info:

VLAN Membership mode: General

Operating parameters:

PVID: 1 (default)

Ingress Filtering: Enabled

Acceptable Frame Type: All

GVRP status: Enabled

Protected: Enabled

Port 1/xg1 is member in:

VLAN	Name	Egress rule	Type
----	-----	-----	-----
1	default	untagged	System
8	VLAN008	tagged	Dynamic
11	VLAN0011	tagged	Static
19	IPv6 VLAN	untagged	Static
72	VLAN0072	untagged	Static

Static configuration:

PVID: 1 (default)

Ingress Filtering: Enabled

Acceptable Frame Type: All

Port 1/xg1 is statically configured to:

VLAN	Name	Egress rule
------	------	-------------

1	default	untagged
---	---------	----------

11	VLAN0011	tagged
----	----------	--------

19	IPv6 VLAN	untagged
----	-----------	----------

72	VLAN0072	untagged
----	----------	----------

Forbidden VLANS:

VLAN	Name
------	------

73	Out
----	-----

Spanning Tree Info

Port 1 (1/xg1) enabled

State: Forwarding Role: Root

Port id: 128.1 Port cost: 20000

Port Fast: No (configured:no)

Designated bridge Priority: 32768 Address:

00:01:42:97:e0:00

Designated port id: 128.25 Designated path cost: 0

BPDU: sent 2, received 120638

show interfaces status

Use the **show interfaces status** command in User EXEC mode to display the status for all configured interfaces.

Syntax

show interfaces status [*ethernet interface* | **port-channel** *port-channel-number*]

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the status for all configured interfaces.

```
console#show interfaces status
```

Port	Type	Duplex	Speed	Neg	Link	Flow Control
					State	Status
1/g1	Gigabit - Level	N/A	Unknown	Auto	Down	Inactive
1/g2	Gigabit - Level	N/A	Unknown	Auto	Down	Inactive
1/g3	Gigabit - Level	N/A	Unknown	Auto	Down	Inactive
1/g4	Gigabit - Level	N/A	Unknown	Auto	Down	Inactive
1/g5	Gigabit - Level	N/A	Unknown	Auto	Down	Inactive
1/g6	Gigabit - Level	N/A	Unknown	Auto	Down	Inactive
1/g7	Gigabit - Level	N/A	Unknown	Auto	Down	Inactive
1/g8	Gigabit - Level	N/A	Unknown	Auto	Down	Inactive

```

1/g9   Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g10  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g11  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g12  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g13  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g14  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g15  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g16  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g17  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g18  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g19  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
--More-- or (q)uit
1/g20  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g21  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g22  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/g23  Gigabit - Level   Full  1000     Auto Up    Inactive
1/g24  Gigabit - Level   N/A   Unknown   Auto Down   Inactive
1/xg1  10G - Level   N/A   Unknown   Auto Down   Inactive
1/xg2  10G - Level   N/A   Unknown   Auto Down   Inactive
1/xg3  10G - Level   N/A   Unknown   Auto Down   Inactive
1/xg4  10G - Level   N/A   Unknown   Auto Down   Inactive

```

```

Ch      Type                                     Link
                                           State
-----
ch1     Link Aggregate                           Down
ch2     Link Aggregate                           Down
ch3     Link Aggregate                           Down
ch4     Link Aggregate                           Down
ch5     Link Aggregate                           Down
ch6     Link Aggregate                           Down
ch7     Link Aggregate                           Down
ch8     Link Aggregate                           Down

```

```

ch9  Link Aggregate          Down
--More-- or (q)uit
ch10 Link Aggregate          Down
ch11 Link Aggregate          Down
ch12 Link Aggregate          Down
ch13 Link Aggregate          Down
ch14 Link Aggregate          Down
ch15 Link Aggregate          Down
ch16 Link Aggregate          Down
ch17 Link Aggregate          Down
ch18 Link Aggregate          Down
ch19 Link Aggregate          Down
ch20 Link Aggregate          Down
ch21 Link Aggregate          Down
ch22 Link Aggregate          Down
ch23 Link Aggregate          Down
ch24 Link Aggregate          Down
ch25 Link Aggregate          Down
ch26 Link Aggregate          Down
ch27 Link Aggregate          Down
ch28 Link Aggregate          Down
ch29 Link Aggregate          Down
ch30 Link Aggregate          Down
ch31 Link Aggregate          Down
ch32 Link Aggregate          Down
--More-- or (q)uit
ch33 Link Aggregate          Down
ch34 Link Aggregate          Down
ch35 Link Aggregate          Down
ch36 Link Aggregate          Down
ch37 Link Aggregate          Down
ch38 Link Aggregate          Down
ch39 Link Aggregate          Down

```

```
ch40 Link Aggregate          Down
ch41 Link Aggregate          Down
ch42 Link Aggregate          Down
ch43 Link Aggregate          Down
ch44 Link Aggregate          Down
ch45 Link Aggregate          Down
ch46 Link Aggregate          Down
ch47 Link Aggregate          Down
ch48 Link Aggregate          Down
```

```
Flow Control:Disabled
```

```
console#
```

The displayed port status information includes the following:

Field	Description
Port	The port number.
Type	The port designated IEEE shorthand identifier. For example 1000Base-T refers to 1000 Mbps baseband signaling including both Tx and Rx transmissions.
Duplex	Displays the port Duplex status.
Speed	Refers to the port speed.
Neg	Describes the Auto-negotiation status.
Link State	Displays the Link Aggregation status.

show statistics ethernet

Use the `show statistics ethernet` command in Privileged EXEC mode to display detailed statistics for a specific port or for the entire switch.

Syntax

```
show statistics ethernet { <unit> / <port-type> <port> | switchport }
```

- unit* — Physical switch identifier within the stack. Values are 1-12.

- *port-type* — Values are **g** for gigabit Ethernet port, or **xg** for 10 gigabit Ethernet port.
- *port* — port number. Values are *1-24* or *1-48* for port_type **g**, and *1-4* for port_type **xg**.
Example: **xg2** is the 10 gigabit Ethernet port 2.
- **switchport** — Displays statistics for the entire switch.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Examples

The following examples show statistics for port **1/g1** and for the entire switch.

```
console#show statistics ethernet 1/g1
Total Packets Received (Octets)..... 779533115
Packets Received 64 Octets..... 48950
Packets Received 65-127 Octets..... 482426
Packets Received 128-255 Octets..... 101084
Packets Received 256-511 Octets..... 163671
Packets Received 512-1023 Octets..... 4824
Packets Received 1024-1518 Octets..... 479543
Packets Received > 1522 Octets..... 0
Packets RX and TX 64 Octets..... 94516
Packets RX and TX 65-127 Octets..... 483312
Packets RX and TX 128-255 Octets..... 101329
Packets RX and TX 256-511 Octets..... 163696
```

```

Packets RX and TX 512-1023 Octets..... 4982
Packets RX and TX 1024-1518 Octets..... 479845
Packets RX and TX 1519-1522 Octets..... 0
Packets RX and TX 1523-2047 Octets..... 0
Packets RX and TX 2048-4095 Octets..... 0
Packets RX and TX 4096-9216 Octets..... 0
Total Packets Received Without Errors..... 1280498
Unicast Packets Received..... 1155457
Multicast Packets Received..... 48339
--More-- or (q)uit
Broadcast Packets Received..... 76702
Total Packets Received with MAC Errors..... 0
Jabbers Received..... 0
Fragments/Undersize Received..... 0
Alignment Errors..... 0
FCS Errors..... 0
Overruns..... 0
Total Received Packets Not Forwarded..... 91
Local Traffic Frames..... 0
802.3x Pause Frames Received..... 0
Unacceptable Frame Type..... 91
Multicast Tree Viable Discards..... 0
Reserved Address Discards..... 0
Broadcast Storm Recovery..... 0
CFI Discards..... 0
Upstream Threshold..... 0
Total Packets Transmitted (Octets)..... 3604988
Packets Transmitted 64 Octets..... 45566
Packets Transmitted 65-127 Octets..... 886

```



```

Packets Transmitted 128-255 Octets..... 245
--More-- or (q)uit
Packets Transmitted 256-511 Octets..... 25
Packets Transmitted 512-1023 Octets..... 158
Packets Transmitted 1024-1518 Octets..... 302
Max Frame Size..... 1518
Total Packets Transmitted Successfully..... 47182
Unicast Packets Transmitted..... 2746
Multicast Packets Transmitted..... 44432
Broadcast Packets Transmitted..... 4
Total Transmit Errors..... 0
FCS Errors..... 0
Tx Oversized..... 0
Underrun Errors..... 0
Total Transmit Packets Discarded..... 0
Single Collision Frames..... 0
Multiple Collision Frames..... 0
Excessive Collision Frames..... 0
Port Membership Discards..... 0
802.3x Pause Frames Transmitted..... 0
GVRP PDUs received..... 0
--More-- or (q)uit
GVRP PDUs Transmitted..... 0
GVRP Failed Registrations..... 0
BPDU: sent 44432, received 0
EAPOL Frames Transmitted..... 0
EAPOL Start Frames Received..... 0
Time Since Counters Last Cleared..... 1 day 0 hr
41 min 44 sec

```

```
console#show statistics ethernet switchport
```

```
Total Packets Received (Octets)..... 16877295
Unicast Packets Received..... 1608
Multicast Packets Received..... 48339
Broadcast Packets Received..... 69535
Receive Packets Discarded..... 0
Octets Transmitted..... 6451988
Packets Transmitted Without Errors..... 91652
Unicast Packets Transmitted..... 2746
Multicast Packets Transmitted..... 88892
Broadcast Packets Transmitted..... 14
Transmit Packets Discarded..... 0
--More-- or (q)uit
Most Address Entries Ever Used..... 141
Address Entries Currently in Use..... 124
Maximum VLAN Entries..... 1024
Most VLAN Entries Ever Used..... 6
Static VLAN Entries..... 6
Dynamic VLAN Entries..... 0
VLAN Deletes..... 0
Time Since Counters Last Cleared..... 1 day 0 hr
42 min 13 sec
console#
```

show storm-control

Use the **show storm-control** command in Privileged EXEC mode to display the configuration of storm control.

Syntax

show storm-control [*all* | *interface*]

- interface* — Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example shows storm control configurations for all valid Ethernet ports. The second example shows flow control mode status.

```
console#show storm-control all
```

Intf	Bcast Mode	Bcast Level	Mcast Mode	Mcast Level	Ucast Mode	Ucast Level
1/g1	Disable	5	Disable	5	Disable	5
1/g2	Disable	5	Disable	5	Disable	5
1/g3	Disable	5	Disable	5	Disable	5
1/g4	Disable	5	Disable	5	Disable	5

```
console#show storm-control
```

```
802.3x Flow Control Mode..... Disable
```

shutdown

Use the **shutdown** command in Interface Configuration mode to disable an interface. To restart a disabled interface, use the **no** form of this command.

Syntax

shutdown

no shutdown

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration (Ethernet, Port-Channel, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Examples

The following example disables Ethernet port 1/g5.

```
console(config)#interface ethernet 1/g5
```

```
console(config-if-1/g5)# shutdown
```

The following example re-enables ethernet port 1/g5.

```
console(config)#interface ethernet 1/g5
```

```
console(config-if-1/g5)# no shutdown
```

speed

Use the **speed** command in Interface Configuration mode to configure the speed of a given Ethernet interface when not using auto-negotiation. To restore the default, use the **no** form of this command.

Syntax

speed [10 | 100]

no speed

- 10 — Configures the port to 10 Mbps operation.
- 100 — Configures the port to 100 Mbps operation.

Default Configuration

This command has no default setting.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the speed operation of Ethernet port 1/g5 to force 100-Mbps operation.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)#speed 100
```

storm-control broadcast

Use the **storm-control broadcast** command in Interface Configuration mode to enable broadcast storm recovery mode for a specific interface. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Syntax

storm-control broadcast [*level* | *rate*]

no storm-control broadcast

- *level*— The configured rate as a percentage of link-speed.
- *rate*— The configured rate in kilobits per second (kbps). (Range: 0-100)

Default Configuration

The default value is 5.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/g1)#storm-control broadcast level  
5
```

storm-control multicast

Use the **storm-control multicast** command in Interface Configuration mode to enable multicast storm recovery mode for an interface. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

When you use the **no storm-control multicast** command to "disable" storm-control after having set the level or rate to a non-default value, that value is still set but is not active until you re-enable storm-control.

Syntax

storm-control multicast [*level* | *rate*]

no storm-control multicast

- *level*— The configured rate as a percentage of link-speed.
- *rate*— The configured rate in kilobits per second (kbps). (Range: 0-100)

Default Configuration

The default value is 5.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/g1)#storm-control multicast level
5
```

storm-control unicast

Use the **storm-control unicast** command in Interface Configuration mode to enable unknown unicast storm control for an interface. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

When you use the **no storm-control multicast** command to "disable" storm-control after having set the level or rate to a non-default value, that value is still set but is not active until you re-enable storm-control.

Syntax

storm-control unicast [*level* | *rate*]

no storm-control unicast

- *level*— The configured rate as a percentage of link-speed.
- *rate* — The configured rate in kilobits per second (kbps). (Range: 0-100)

Default Configuration

The default value is 5.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/g1)#storm-control unicast level 5
```


GVRP Commands

This chapter explains the following commands:

- clear gvrp statistics
- garp timer
- gvrp enable (global)
- gvrp enable (interface)
- gvrp registration-forbid
- gvrp vlan-creation-forbid
- show gvrp configuration
- show gvrp error-statistics
- show gvrp statistics

clear gvrp statistics

Use the `clear gvrp statistics` command in Privileged EXEC mode to clear all the GVRP statistics information.

Syntax

`clear gvrp statistics [ethernet interface | port-channel port-channel-number]`

- *interface* — A valid Ethernet interface.
- *port-channel-number* — A valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example clears all the GVRP statistics information on port 1/g8.

```
console# clear gvrp statistics ethernet 1/g8
```

garp timer

Use the `garp timer` command in Interface Configuration mode to adjust the GARP application join, leave, and leaveall GARP timer values. To reset the timer to default values, use the **no** form of this command.

Syntax

`garp timer {join | leave | leaveall} timer_value`

`no garp timer`

- **join** — Indicates the time in centiseconds that PDUs are transmitted.

- **leave** — Indicates the time in centiseconds that the device waits before leaving its GARP state.
- **leaveall** — Used to confirm the port within the VLAN. The time is the interval between messages sent, measured in centiseconds.
- *timer_value* — Timer values in centiseconds. The range is 10-100 for **join**, 20-600 for **leave**, and 200-6000 for **leaveall**.

Default Configuration

The default timer values are as follows:

- Join timer — 20 centiseconds
- Leave timer — 60 centiseconds
- Leaveall timer — 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

The following *relationships* for the various timer values must be maintained:

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on Layer 2-connected devices, the GARP application will not operate successfully.

The *timer_value* setting must be a multiple of 10.

Example

The following example sets the leave timer for port 1/g8 to 90 centiseconds.

```
console (config)# interface ethernet 1/g8
```

```
console (config-if-1/g8)# garp timer leave 90
```

gvrp enable (global)

Use the **gvrp enable (global)** command in Global Configuration mode to enable GVRP globally on the switch. To disable GVRP globally on the switch, use the **no** form of this command.

Syntax

gvrp enable
no gvrp enable

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example globally enables GVRP on the device.

```
console(config)#gvrp enable
```

gvrp enable (interface)

Use the **gvrp enable** command in Interface Configuration mode to enable GVRP on an interface. To disable GVRP on an interface, use the **no** form of this command.

Syntax

gvrp enable
no gvrp enable

Default Configuration

GVRP is disabled on all interfaces by default.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

An Access port cannot join dynamically to a VLAN because it is always a member of only one VLAN.

Membership in untagged VLAN would be propagated in a same way as a tagged VLAN. In such cases it is the administrator's responsibility to set the PVID to be the untagged VLAN VID.

Example

The following example enables GVRP on ethernet 1/g8.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#gvrp enable
```

gvrp registration-forbid

Use the **gvrp registration-forbid** command in Interface Configuration mode to deregister all VLANs on a port and prevent any dynamic registration on the port. To allow dynamic registering for VLANs on a port, use the **no** form of this command.

Syntax

```
gvrp registration-forbid
no gvrp registration-forbid
```

Default Configuration

Dynamic registering and deregistering for each VLAN on the port is not forbidden.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how default dynamic registering and deregistering is forbidden for each VLAN on port 1/g8.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#gvrp registration-forbid
```

gvrp vlan-creation-forbid

Use the **gvrp vlan-creation-forbid** command in Interface Configuration mode to disable dynamic VLAN creation. To disable dynamic VLAN creation, use the **no** form of this command.

Syntax

```
gvrp vlan-creation-forbid
no gvrp vlan-creation-forbid
```

Default Configuration

By default, dynamic VLAN creation is enabled.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example disables dynamic VLAN creation on port 1/g8.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#gvrp vlan-creation-forbid
```

show gvrp configuration

Use the **show gvrp configuration** command in Privileged EXEC mode to display GVRP configuration information. Timer values are displayed. Other data shows whether GVRP is enabled and which ports are running GVRP.

Syntax

show gvrp configuration [*ethernet interface* | *port-channel port-channel-number*]

- *interface* — A valid Ethernet interface.
- *port-channel-number* — A valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display GVRP configuration information:

```
console# show gvrp configuration
```

```
Global GVRP Mode: Disabled
```

Join	Leave	LeaveAll	Port	VLAN
Interface	Timer	Timer	Timer	GVRP Mode
Create Register				
	(centisecs)	(centisecs)	(centisecs)	
Forbid	Forbid			
-----	-----	-----	-----	-----
1/g1	20	60	1000	Disabled

1/g2	20	60	1000	Disabled
1/g3	20	60	1000	Disabled
1/g4	20	60	1000	Disabled
1/g5	20	60	1000	Disabled
1/g6	20	60	1000	Disabled
1/g7	20	60	1000	Disabled
1/g8	20	60	1000	Disabled
1/g9	20	60	1000	Disabled
1/g10	20	60	1000	Disabled
1/g11	20	60	1000	Disabled
1/g12	20	60	1000	Disabled
1/g13	20	60	1000	Disabled
1/g14	20	60	1000	Disabled

show gvrp error-statistics

Use the `show gvrp error-statistics` command in User EXEC mode to display GVRP error statistics.

Syntax

`show gvrp error-statistics [ethernet interface | port-channel port-channel-number]`

- *interface* — A valid Ethernet interface.
- *port-channel-number* — A valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays GVRP error statistics information.

```
console>show gvrp error-statistics
```

GVRP error statistics:

Legend:

INVPROT: Invalid Protocol Id INVATYP: Invalid
Attribute Type
INVALEN: Invalid Attribute Length INVAVAL: Invalid
Attribute Value
INVEVENT: Invalid Event

Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT
----	-----	-----	-----	-----	-----
1/g1	0	0	0	0	0
1/g2	0	0	0	0	0
1/g3	0	0	0	0	0
1/g4	0	0	0	0	0

show gvrp statistics

Use the `show gvrp statistics` command in User EXEC mode to display GVRP statistics.

Syntax

`show gvrp statistics [ethernet interface | port-channel port-channel-number]`

- *interface* — A valid Ethernet interface.
- *port-channel-number* — A valid port channel index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

This example shows output of the `show gvrp statistics` command.

```
console>show gvrp statistics
```

```
GVRP statistics:
```

```
-----
```

```
Legend:
```

```
rJE  : Join Empty Received
rEmp : Empty Received
rLE  : Leave Empty Received
sJE  : Join Empty Sent
sEmp : Empty Sent
sLE  : Leave Empty Sent
```

```
rJIn : Join In Received
rLIn : Leave In Received
rLA  : Leave All Received
JIn  : Join In Sent
sLIn : Leave In Sent
sLA  : Leave All Sent
```

Port	rJE	rJIn	rEmp	rLin	rLE	rLA	sJE	sJIn	sEmp	sLin	sLE	sLA
----	---	----	----	----	---	---	---	---	---	----	----	----
1/g1	0	0	0	0	0	0	0	0	0	0	0	0
1/g2	0	0	0	0	0	0	0	0	0	0	0	0
1/g3	0	0	0	0	0	0	0	0	0	0	0	0
1/g4	0	0	0	0	0	0	0	0	0	0	0	0
1/g5	0	0	0	0	0	0	0	0	0	0	0	0
1/g6	0	0	0	0	0	0	0	0	0	0	0	0
1/g7	0	0	0	0	0	0	0	0	0	0	0	0
1/g8	0	0	0	0	0	0	0	0	0	0	0	0

IGMP Snooping Commands

This chapter explains the following commands:

- ip igmp snooping (global)
- ip igmp snooping (interface)
- ip igmp snooping host-time-out
- ip igmp snooping leave-time-out
- ip igmp snooping mrouter-time-out
- show ip igmp snooping groups
- show ip igmp snooping interface
- show ip igmp snooping mrouter
- ip igmp snooping (VLAN)
- ip igmp snooping fast-leave
- ip igmp snooping groupmembership-interval
- ip igmp snooping maxresponse
- ip igmp snooping mcertexpiretime

ip igmp snooping (global)

Use the **ip igmp snooping** command in Global Configuration mode to globally enable Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable IGMP snooping globally.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping is enabled on static VLANs only and is not enabled on Private VLANs or their community VLANs.

Example

The following example enables IGMP snooping.

```
console(config)# ip igmp snooping
```

ip igmp snooping (interface)

Use the **ip igmp snooping** command in Interface Configuration mode to enable Internet Group Management Protocol (IGMP) snooping on a specific interface. To disable IGMP snooping on an Ethernet interface, use the **no** form of this command.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

IGMP snooping can be enabled on Ethernet interfaces.

Example

The following example enables IGMP snooping.

```
console(config-if-1/g1)#ip igmp snooping
```

ip igmp snooping host-time-out

Use the **ip igmp snooping host-time-out** command in Interface Configuration mode to configure the host-time-out. If an IGMP report for a Multicast group is not received for a host time-out period from a specific port, this port is deleted from the member list of that Multicast group. To reset to the default host time-out, use the **no** form of this command.

Syntax

ip igmp snooping host-time-out *time-out*

no ip igmp snooping host-time-out

- *time-out* — Host timeout in seconds. (Range: 2- 3600)

Default Configuration

The default host-time-out is 260 seconds.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The timeout should be more than sum of response time and twice the query interval.

Example

The following example configures the host timeout to 300 seconds.

```
console(config-if-1/g1)#ip igmp snooping host-time-out 300
```

ip igmp snooping leave-time-out

Use the **ip igmp snooping leave-time-out** command in Interface Configuration mode to configure the leave-time-out. If an IGMP report for a Multicast group is not received within the leave-time-out period after an IGMP leave was received from a specific port, the current port is deleted from the member list of that Multicast group. To configure the default leave-time-out, use the **no** form of this command.

Syntax

ip igmp snooping leave-time-out [*time-out* / *immediate-leave*]

no ip igmp snooping leave-time-out

- *time-out* — Specifies the leave-time-out in seconds. (Range: 1 - 3174)
- *immediate-leave* — Specifies that the port should be removed immediately from the members list after receiving IGMP Leave.

Default Configuration

The default leave-time-out configuration is 10 seconds.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The leave timeout should be set greater than the maximum time that a host is allowed to respond to an IGMP Query.

Use **immediate leave** only where there is only one host connected to a port.

Example

The following example configures the host leave-time-out to 60 seconds.

```
console(config-if-1/g1)#ip igmp snooping leave-time-out 60
```

ip igmp snooping mrouter-time-out

Use the **ip igmp snooping mrouter-time-out** command in Interface Configuration mode to configure the mrouter-time-out. This command is used for setting the aging-out time after Multicast router ports are automatically learned. To reset to the default mrouter-time-out, use the **no** form of this command.

Syntax

ip igmp snooping mrouter-time-out *time-out*

no ip igmp snooping mrouter-time-out

- *time-out* — mrouter timeout in seconds for IGMP. (Range: 1–3600)

Default Configuration

The default value is 300 seconds.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the mrouter timeout to 200 seconds.

```
console(config-if-1/g1)#ip igmp snooping mrouter-  
time-out 200
```

show ip igmp snooping groups

Use the `show ip igmp snooping groups` command in User EXEC mode to display the Multicast groups learned by IGMP snooping.

Syntax

`show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address]`

- *vlan_id* — Specifies a VLAN ID value.
- *ip-multicast-address* — Specifies an IP Multicast address.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

To see the full Multicast address table (including static addresses) use the `show bridge address-table` command.

Example

The example shows Multicast groups learned by IGMP snooping for all VLANs.

```
console>show ip igmp snooping groups
```

Vlan	IP Address	Ports
----	-----	-----
1	224-239.130 2.2.3	1/g1, 2/g2
19	224-239.130 2.2.8	1/g9-g11

IGMP Reporters that are forbidden statically:

Vlan	IP Address	Ports

1	224-239.130 2.2.3	1/g19

show ip igmp snooping interface

Use the `show ip igmp snooping interface` command in Privileged EXEC mode to display the IGMP snooping configuration.

Syntax

`show ip igmp snooping interface interface {ethernet interface | port-channel port-channel-number}`

- *interface* — Valid Ethernet port. The full syntax is *unit/port*.
- *port-channel-number* — Valid port-channel index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The example displays IGMP snooping information.

```
console#show ip igmp snooping interface 1/g1
Slot/Port..... 1/g1
IGMP Snooping Admin Mode..... Disabled
```

```
Fast Leave Mode..... Disabled
Group Membership Interval..... 260
Max Response Time..... 10
Multicast Router Present Expiration Time.. 300
```

show ip igmp snooping mrouter

Use the **show ip igmp snooping mrouter** command in Privileged EXEC mode to display information on dynamically learned Multicast router interfaces.

Syntax

show ip igmp snooping mrouter

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows IGMP snooping mrouter information.

```
console#show igmp snooping mrouter
```

```
Port.....1/g1
```

ip igmp snooping (VLAN)

Use the **ip igmp snooping** command in VLAN Configuration mode to enable IGMP snooping on a particular interface or on all interfaces participating in a VLAN. To disable IGMP snooping use the **no** form of this command.

Syntax

ip igmp snooping *vlan-id*

no ip igmp snooping

Default Configuration

IGMP snooping is disabled on VLAN interfaces by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IGMP snooping on VLAN 2.

```
console(config-vlan)#ip igmp snooping 2
```

ip igmp snooping fast-leave

This command enables or disables IGMP Snooping fast-leave mode on a selected VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface. The **no** form of this command disables IGMP Snooping fast-leave mode on a VLAN.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This setting prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Syntax

`ip igmp snooping fast-leave vlan-id`

`no ip igmp snooping fast-leave`

- *vlan id* — Number assigned to the VLAN.

Default Configuration

IGMP snooping fast-leave mode is disabled on VLANs by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IGMP snooping fast-leave mode on VLAN 2.

```
console(config-vlan)#ip igmp snooping fast-leave 2
```

ip igmp snooping groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds. The **no** form of this command sets the IGMPv3 Group Membership Interval time to the default value.

Syntax

`ip igmp snooping groupmembership-interval vlan-id seconds`

`no ip igmp snooping groupmembership-interval`

- *vlan-id* — Number assigned to the VLAN
- *seconds* — IGMP group membership interval time in seconds. (Range: 2–3600)

Default Configuration

The default group membership interval time is 260 seconds.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures an IGMP snooping group membership interval of 520 seconds.

```
console(config-vlan)#ip igmp snooping  
groupmembership-interval 2 520
```

ip igmp snooping maxresponse

This command sets the IGMP Maximum Response time on a particular VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 3174 seconds. The **no** form of this command sets the maximum response time on the VLAN to the default value.

Syntax

ip igmp snooping maxresponse *vlan-id seconds*

no ip igmp snooping maxresponse *vlan-id*

- *vlan-id* — Number assigned to the VLAN.
- *seconds* — IGMP Maximum response time in seconds. (Range: 1-3174)

Default Configuration

The default maximum response time is 10 seconds.

Command Mode

VLAN Configuration mode

User Guidelines

When using IGMP Snooping Querier, this parameter should be less than the value for the IGMP Snooping Querier query interval.

Example

The following example sets the maximum response time to 60 seconds on VLAN 2.

```
console(config-vlan)#ip igmp snooping maxresponse 2  
60
```

ip igmp snooping mcrtexpiretime

This command sets the Multicast Router Present Expiration time. The time is set on a particular VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 1–2147483647 seconds. A value of 0 indicates an infinite time-out (no expiration). The **no** form of this command sets the Multicast Router Present Expiration time to 0. The time is set for a particular VLAN.

Syntax

ip igmp snooping mcrtexpiretime *vlan-id seconds*

no ip igmp mcrtexpiretime *vlan-id*

- *vlan id*— Number assigned to the VLAN
- *seconds*— Multicast router present expiration time. (Range: 1–3600)

Default Configuration

The default multicast router present expiration time is 300 seconds.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the multicast router present expiration time on VLAN 2 to 60 seconds.

```
console(config-vlan)#ip igmp mcrtexpiretime 2 60
```


IGMP Snooping Querier Commands

This chapter explains the following commands:

- `ip igmp snooping querier`
- `ip igmp snooping querier election participate`
- `ip igmp snooping querier query-interval`
- `ip igmp snooping querier timer expiry`
- `ip igmp snooping querier version`
- `show igmp snooping querier`

ip igmp snooping querier

This command enables or disables IGMP Snooping Querier on the system (Global Configuration mode) or on a VLAN. Using this command, you can specify the IP address that the snooping querier switch should use as the source address when generating periodic queries. The **no** form of this command disables IGMP Snooping Querier on the system. Use the optional **address** parameter to reset the querier address to 0.0.0.0.

If a VLAN has IGMP Snooping Querier enabled, and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping querier functionality is re-enabled if IGMP Snooping is operational on the VLAN.

The IGMP Snooping Querier application sends periodic general queries on the VLAN to solicit membership reports.

Syntax

ip igmp snooping querier [*vlan-id*] [*address ipv4_address*]

no igmp snooping querier [*vlan-id*] [*address*]

- *vlan-id* — A valid VLAN number.
- *ipv4_address* — An IPv4 address used for the source address.

Default Configuration

IGMP snooping querier is disabled by default.

Command Mode

Global Configuration mode

VLAN Configuration mode

User Guidelines

When using the command in Global Configuration mode to configure a snooping querier source address, the IPv4 address is the global querier address. When using the command in VLAN Configuration mode to configure a snooping querier source address, the IPv4 address is the querier address for the VLAN. If there are no global or VLAN querier addresses

configured, then use the management IP address as the IGMP snooping querier source address. Using all zeros for the querier IP address removes it. The VLAN IP address takes precedence over the global IP address.

Example

The following example enables IGMP snooping querier in VLAN Configuration mode.

```
console(config-vlan)#ip igmp snooping querier 1  
address 10.19.67.1
```

ip igmp snooping querier election participate

This command enables the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier source address is more than the Snooping Querier address, it stops sending periodic queries. If the Snooping Querier wins the election, then it continues sending periodic queries. The **no** form of this command sets the snooping querier not to participate in the querier election but to go into a non-querier mode as soon in as it discovers the presence of another querier in the same VLAN.

Syntax

ip igmp snooping querier election participate *vlan-id*

no ip igmp snooping querier election participate *vlan-id*

Default Configuration

The snooping querier is configured to not participate in the querier election by default.

Command Mode

VLAN Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the snooping querier to participate in the querier election.

```
console(config-vlan)#ip igmp snooping querier  
election participate
```

ip igmp snooping querier query-interval

This command sets the IGMP Querier Query Interval time, which is the amount of time in seconds that the switch waits before sending another periodic query. The no form of this command sets the IGMP Querier Query Interval time to its default value.

Syntax

ip igmp snooping querier query-interval *seconds*

no ip igmp snooping querier query-interval

- *seconds* — Amount of time in seconds that the switch waits before sending another general query. (Range: 1-1800)

Default Configuration

The query interval default is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

The value of this parameter should be larger than the IGMP Snooping Max Response Time.

Example

The following example sets the query interval to 1800:

```
ip igmp snooping querier query_interval 1800
```

ip igmp snooping querier timer expiry

This command sets the IGMP Querier timer expiration period which is the time period that the switch remains in Non-Querier mode after it has discovered that there is a Multicast Querier in the network. The **no** form of this command sets the IGMP Querier timer expiration period to its default value.

Syntax

ip igmp snooping querier timer expiry *seconds*

no ip igmp snooping querier timer expiry

- *seconds* — The time in seconds that the switch remains in Non-Querier mode after it has discovered that there is a multicast querier in the network. The range is 60–300 seconds.

Default Configuration

The query interval default is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the querier timer expiry time to 100 seconds.

```
ip igmp snooping querier timer expiry 100
```

ip igmp snooping querier version

This command sets the IGMP version of the query that the snooping switch is going to send periodically. The **no** form of this command sets the IGMP Querier Version to its default value.

Syntax

`ip igmp snooping querier version number`

`no ip igmp snooping querier version`

- *number* — IGMP version. (Range: 1–2)

Default Configuration

The querier version default is 2.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the IGMP version of the querier to 1.

```
ip igmp snooping querier version 1
```

show igmp snooping querier

This command displays IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

When the optional argument *vlan_id* is not used, the command shows the following information:

- Admin Mode — Indicates whether or not IGMP Snooping Querier is active on the switch.
- Admin Version — Indicates the version of IGMP that will be used while sending out the queries.
- Source IP Address — Shows the IP address that is used in the IPv4 header when sending out IGMP queries. It can be configured using the appropriate command.
- Query Interval — Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query

- **Querier Timeout** — Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlan_id*, the following information appears:

- **VLAN Admin Mode** — Indicates whether IGMP Snooping Querier is active on the VLAN.
- **VLAN Operational State** — Indicates whether IGMP Snooping Querier is in the Querier or Non-Querier state. When the switch is in Querier state it sends out periodic general queries. When in Non-Querier state it waits for moving to Querier state and does not send out any queries.
- **VLAN Operational Max Response Time** — Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
- **Querier Election Participate** — Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
- **Last Querier Address** — Indicates the IP address of the most recent Querier from which a Query was received.
- **Last Querier Version** — Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.
- **Elected Querier** — Indicates the IP address of the Querier that has been designated as the Querier based on its source IP address. This field will be 0.0.0.0 when Querier Election Participate mode is disabled

When the optional argument *detail* is used, the command shows the global information and the information for all Querier enabled VLANs.

Syntax

show ip igmp snooping querier [{*detail* | *vlan* *vlan_id*}]

- *vlan_id* — Number assigned to the VLAN.

Default Configuration

This command has no default configuration

Command Mode

Privileged Exec mode

User Guidelines

This command has no user guidelines.

Example

The following example shows querier information for VLAN 2.

```
console#show ip igmp snooping querier vlan 2
```

```
Vlan 2 :    IGMP Snooping querier status
```

```
-----  
IGMP Snooping Querier Vlan Mode..... Disable  
Querier Election Participate Mode..... Disable  
Querier Vlan Address..... 0.0.0.0  
Operational State..... Disabled  
Operational version..... 2
```

IP Addressing Commands

This chapter explains the following commands:

- clear host
- ip address
- ip address dhcp
- ip address vlan
- ip default-gateway
- ip domain-lookup
- ip domain-name
- ip host
- ip name-server
- ipv6 address
- ipv6 enable
- ipv6 gateway
- show arp switch
- show hosts
- show ip helper-address
- show ip interface management

clear host

Use the **clear host** command in Privileged EXEC mode to delete entries from the host name-to-address cache.

Syntax

clear host {*name* | *}

- *name* — Host name to be deleted from the host name-to-address cache. (Range: 1-255 characters)
- * — Deletes all entries in the host name-to-address cache.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example deletes all entries from the host name-to-address cache.

```
console#clear host *
```

ip address

Use the **ip address** command in Global Configuration mode to set an IP address. To remove an IP address, use the **no** form of this command.

Syntax

ip address *ip-address* {*mask* | *prefix-length*}

no ip address

- *ip-address* — Specifies a valid IP address.

- *mask* — Specifies a valid subnet (network) mask IP address.
- *prefix-length* — The number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 1-30)

Default Configuration

The switch management interface obtains an IP address via DHCP by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Examples

The following examples configure the IP address 131.108.1.27 and subnet mask 255.255.255.0 and the same IP address with prefix length of 24 bits.

```
console(config)#ip address 131.108.1.27 255.255.255.0
console(config)#ip address 131.108.1.27 /24
```

ip address dhcp

Use the **ip address dhcp** command in Global Configuration mode to acquire an IP address for management interface from the Dynamic Host Configuration Protocol (DHCP) server. To deconfigure any acquired address, use the **no** form of this command.

Syntax

ip address {dhcp|bootp|none}

- **dhcp**--Sets protocol to dhcp
- **bootp**--Sets protocol to bootp
- **none**--No protocol is set

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The **ip address dhcp** command allows the switch to dynamically obtain an IP address by using the DHCP protocol.

Example

The following example acquires an IP address for the switch management interface from DHCP.

```
console(config)#ip address dhcp
```

ip address vlan

Use the **ip address vlan** command in Global Configuration mode to set the management VLAN.

Syntax

ip address vlan *vlanid*

no ip address vlan

- *vlanid* — vlan identification. (Range 1–4093)

Default Configuration

The default configuration value is 1.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets VLAN 5 as management VLAN.

```
console(config)#ip address vlan 5
```

ip default-gateway

Use the **ip default-gateway** command in Global Configuration mode to define a default gateway (router).

Syntax

ip default-gateway *ip-address*

- *ip-address* — Valid IP address that specifies the IP address of the default gateway.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

A static IP address must be configured using the **ip address** command before setting the default gateway. The default gateway should reside on the subnet defined by the **ip address** command.



NOTE: For management traffic forwarding decisions, a default-route configured on the switch (CLI, Web, SNMP, or learned via routing protocol such as OSPF), takes precedence over the **ip default-gateway** setting.

Example

The following example defines ip default-gateway as 10.240.4.1.

```
console(config)#ip default-gateway 10.240.4.1
```

ip domain-lookup

Use the **ip domain-lookup** command in Global Configuration mode to enable IP Domain Naming System (DNS)-based host name-to-address translation. To disable the DNS, use the **no** form of this command.

Syntax

ip domain-lookup

no ip domain-lookup

Default Configuration

The DNS is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the IP Domain Naming System (DNS)-based host name-to-address translation.

```
console(config)#ip domain-lookup
```

ip domain-name

Use the **ip domain-name** command in Global Configuration mode to define a default domain name used to complete unqualified host names. To delete the default domain name, use the **no** form of this command.

Syntax

ip domain-name *name*

no ip domain-name

- *name* — Default domain name used to complete an unqualified host name. Do not include the initial period that separates the unqualified host name from the domain name (Range: 1-255 characters).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a default domain name of dell.com.

```
console(config)#ip domain-name dell.com
```

ip host

Use the **ip host** command in Global Configuration mode to define static host name-to-address mapping in the host cache. To delete the name-to-address mapping, use the **no** form of this command.

Syntax

ip host *name address*

no ip host *name*

- *name* — Host name.
- *address* — IP address of the host.

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a static host name-to-address mapping in the host cache.

```
console(config)#ip host accounting.dell.com
176.10.23.1
```

ip name-server

Use the **ip name-server** command in Global Configuration mode to define available IPv4 or IPv6 name servers. To delete a name server, use the **no** form of this command.

Syntax

ip name-server *server-address1* [*server-address2* ... *server-address8*]

no ip name-server [*server-address1* ... *server-address8*]

- *server-address*—Valid IPv4 or IPv6 addresses of the name server. (Range: 1–255 characters)

Default Configuration

No name server IP addresses are specified.

Command Mode

Global Configuration mode

User Guidelines

Server preference is determined by entry order.

Up to eight servers can be defined in one command or by using multiple commands.

Example

The following example sets the available name server.

```
console (config) #ip name-server 176.16.1.18
```

ipv6 address

Use the **ipv6 address** command to set the IPv6 address of the management interface. Use the "no" form of this command to reset the IPv6 address to the default.

Syntax

ipv6 address {*prefix/prefix-length* [*eui64*] | **autoconfig** | **dhcp**}

no ipv6 address

- *prefix*—Consists of the bits of the address to be configured.
- *prefix-length*—Designates how many of the high-order contiguous bits of the address make up the prefix.
- *eui64*—The optional eui-64 field designates that IPv6 processing on the interfaces is enabled using an EUI-64 interface ID in the low order 64 bits of the address. If this option is used, the value of *prefix_length* must be 64 bits.
- **autoconfig**—Use this keyword to set the IPv6 address auto configuration mode.
- **dhcp**—Use this keyword to obtain an IPv6 address via DHCP.

Default Configuration

There is no IPv6 address configured by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 address dhcp
```

```
console(config)#ipv6 address autoconfig
```

```
console(config)#ipv6 address 2003::6/64
```

```
console(config)#ipv6 address 2001::/64 eui64
```

```
console(config)#no ipv6 address dhcp
```

```
console(config)#no ipv6 address autoconfig
```

```
console(config)#no ipv6 address 2003::6/64
```

```
console(config)#no ipv6 address 2001::/64 eui64
```

```
console(config)#no ipv6 address
```

ipv6 enable

Use the **ipv6 enable** command to enable IPv6 on the management interface. Use the "no" form of this command to disable IPv6 on the management interface.

Syntax

```
ipv6 enable
```

```
no ipv6 enable
```

Default Configuration

IPv6 is enabled on the management interface by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#no ipv6 enable
```

ipv6 gateway

Use the **ipv6 gateway** command to configure an IPv6 gateway for the management interface. Use the "no" form of this command to reset the gateway to the default.

Syntax

ipv6 gateway *gateway-address*

no ipv6 gateway

gateway-address—The gateway address in IPv6 global or link-local address format.

Default Configuration

There is no IPv6 gateway configured by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 gateway 2003::1
```

```
console(config)#no ipv6 gateway
```

show arp switch

Use the **show arp switch** command in Privileged EXEC mode to display the ARP cache entries learned on the management port.

Syntax

```
show arp switch
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Note that this command only show ARP entries used by the management interface. It is logically separate from the ARP table used by the routing interfaces. See the **show arp** command for details on how to view ARP entries for the routing interfaces.

Example

The following example displays ARP table information.

```
console#show arp switch
```

MAC Address	IP Address	Interface
0016.9CE1.D800	10.27.6.1	1/g37

show hosts

Use the **show hosts** command in User EXEC mode to display the default domain name, a list of name server hosts, and the static and cached list of host names and addresses. The command itself shows hosts [hostname].

- Host name. (Range: 1–255 characters)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about IP hosts.

```
console>show hosts
Host name:
Default domain: gm.com, sales.gm.com, usa.sales.gm.com
Name/address lookup is enabled
Name servers (Preference order): 176.16.1.18 176.16.1.19
Configured host name-to-address mapping:
Host                               Addresses
-----
accounting.gm.com                  176.16.8.8
Cache:                             TTL (Hours)
Host                               Total      Elapsed    Type      Addresses
-----
www.stanford.edu                   72         3          IP        171.64.14.203
```

show ip helper-address

Use the `show ip helper-address` command in Privileged EXEC mode to display IP helper addresses configuration.

Syntax

`show ip helper-address [intf-address]`

- intf-address* — IP address of a routing interface. (Range: Any valid IP address)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#show ip helper-address
```

```
IP helper is enabled
```

Interface	UDP Port	Discard	Hit Count	Server Address
-----	-----	-----	-----	-----
vlan 25	domain	No	0	192.168.40.2
vlan 25	dhcp	No	0	192.168.40.2
vlan 30	dhcp	Yes	0	
vlan 30	162	No	0	192.168.23.1
Any	dhcp	No	0	192.168.40.1

show ip interface management

Use the **show ip interface management** command to display the management interface configuration.

Syntax

show ip interface management

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the management interface configuration.

```
console#show ip interface management
```

```
IP Address..... 10.27.21.52
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.27.21.1
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is..... FE80::2FF:F2FF:FEA3:7777/64
IPv6 Gateway..... none
Burned In MAC Address..... 00:FF:F2:A3:77:77
Configured IPv4 Protocol..... DHCP
Configured IPv6 Protocol..... None
IPv6 AutoConfig Mode..... Disabled
Management VLAN ID..... 1
```


IPv6 Access List Commands

This chapter explains the following commands:

- {deny | permit}
- ipv6 access-list
- ipv6 access-list rename
- ipv6 traffic-filter
- show ipv6 access-lists

{deny | permit}

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the 'every' keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword 'any' to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The assign-queue parameter is valid only for a permit rule.

Syntax

```
{permit | deny} {every | {{icmp | igmp | ipv6 | tcp | udp | number} {any  
| source ipv6 prefix/prefix length} [eq {portkey | portvalue}] {any |  
destination ipv6 prefix/prefix length} [eq {portkey | portvalue}] [flow-label  
value] [dscp dscp]}} [log] [assign-queue queue-id] [{mirror | redirect}  
interface]
```

- **deny | permit** — Specifies whether the IP ACL rule permits or denies an action.
- **every** — Allows all protocols.
- **number** — Standard protocol number or protocol keywords **icmp**, **igmp**, **ipv6**, **tcp**, **udp**.
- **source ipv6 prefix** — IPv6 prefix in IPv6 global address format.
- **prefix-length** — IPv6 prefix length value.
- **eq** — Equal. Refers to the Layer 4 port number being used as a match criteria. The first reference is source match criteria, the second is destination match criteria.
- **portkey** — Or you can specify the portkey, which can be one of the following keywords: **domain**, **echo**, **efts**, **ftpdata**, **http**, **smtp**, **snmp**, **telnet**, **fttp**, and **www**.

- *portvalue* — The source layer 4 port match condition for the ACL rule is specified by the port value parameter. (Range: 0–65535).
- *destination ipv6 prefix* — IPv6 prefix in IPv6 global address format.
- **flow label value** — The value to match in the Flow Label field of the IPv6 header (Range 0–1048575).
- **dscp dscp** — Specifies the TOS for an IPv6 ACL rule depending on a match of DSCP values using the parameter dscp.
- **log** — Specifies that this rule is to be logged.
- **assign-queue queue-id** — Specifies particular hardware queue for handling traffic that matches the rule. (Range: 0-6)
- **mirror interface** — Allows the traffic matching this rule to be copied to the specified interface.
- **redirect interface** — This parameter allows the traffic matching this rule to be forwarded to the specified interface.

Default Configuration

This command has no default configuration.

Command Mode

Ipv6-Access-List Configuration mode

User Guidelines

Users are permitted to add rules, but if a packet does not match any user-specified rules, the packet is dropped by the implicit “deny all” rule.

The 'no' form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and re specified.

Example

The following example creates rules in an IPv6 ACL named "STOP_HTTP" to discard any HTTP traffic from the 2001:DB8::/32 network, but allow all other traffic from that network:

```
console(config)#ipv6 access-list STOP_HTTP
```

```
console(Config-ipv6-acl)#deny ipv6 2001:DB8::/32 any
eq http

console(Config-ipv6-acl)#permit ipv6 2001:DB8::/32
any

console(Config-ipv6-acl)#
```

ipv6 access-list

The **ipv6 access-list** command creates an IPv6 Access Control List (ACL) consisting of classification fields defined for the IP header of an IPv6 frame. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

If an IPv6 ACL with this name already exists, this command enters Ipv6-Access-List config mode to update the existing IPv6 ACL.

Use the “no” form of the command to delete an IPv6 ACL from the system.

Syntax

ipv6 access-list *name*

no ipv6 access-list *name*

- *name* — Alphanumeric string of 1 to 31 characters uniquely identifying the IPv6 access list.

Default Configuration

There is no default configuration for this command.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command

Example

The following example creates an IPv6 ACL named "DELL_IP6" and enters the IPv6-Access-List Config mode:

```
console(config)#ipv6 access-list DELL_IP6
console(Config-ipv6-acl)#
```

ipv6 access-list rename

The **ipv6 access-list rename** command changes the name of an IPv6 Access Control List (ACL). This command fails if an IPv6 ACL with the new name already exists.

Syntax

ipv6 access-list rename *name newname*

- *name* — the name of an existing IPv6 ACL.
- *newname* — alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

Default Configuration

There is no default configuration for this command.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(Config)#ipv6 access-list rename DELL_IP6
DELL_IP6_NEW_NAME
```

ipv6 traffic-filter

The **ipv6 traffic-filter** command either attaches a specific IPv6 Access Control List (ACL) to an interface or associates it with a VLAN ID in a given direction.

An optional sequence number may be specified to indicate the order of this access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified IPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

Use the “no” form of the command to remove an IPv6 ACL from the interface(s) in a given direction.

Syntax

ipv6 traffic-filter *name direction* [**sequence** *seq-num*]

no ipv6 traffic-filter *name direction*

- **name** — Alphanumeric string of 1 to 31 characters uniquely identifying the IPv6 access list.
- **direction** — Direction of the ACL. (Range: **in** or **out**)
- **sequence** *seq-num* — Order of access list relative to other access lists already assigned to this interface and direction. (Range: 1–4294967295)

Default Configuration

This command has no default configuration.

Command Modes

Global Configuration mode

Interface Configuration (Ethernet, Port-channel, VLAN) mode

User Guidelines

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces.

Example

The following example attaches an IPv6 access control list to an interface.

```
console (config-if-1/g1) #ipv6 traffic-filter DELL_IP6
in
```

show ipv6 access-lists

The `show ipv6 access-lists` command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the [name] parameter to identify a specific IPv6 ACL to display.

Syntax

```
show ipv6 access-lists [name]
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays configuration information for the IPv6 ACLs.

```
console#show ipv6 access-lists
```

Current number of all ACLs: 1 Maximum number of all ACLs: 100

IPv6 ACL Name VLAN(s)	Rules	Direction	Interface(s)

STOP_HTTP	2	inbound	1/g1

console#show ipv6 access-lists STOP_HTTP

ACL Name: STOP_HTTP

Inbound Interface(s): 1/g1

Rule Number: 1

Action..... deny
Protocol..... 255(ipv6)
Source IP Address..... 2001:DB8::/32
Destination L4 Port Keyword..... 80(www/http)

Rule Number: 2

Action..... permit
Protocol..... 255(ipv6)
Source IP Address..... 2001:DB8::/32

The command output provides the following information:

Field	Description
Rule Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	Displays the action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	This displays the protocol to filter for this rule.
Source IP Address	This displays the source IP address for this rule.
Source L4 Port Keyword	This field displays the source port for this rule.
Destination IP Address	This displays the destination IP address for this rule.

Destination L4 Port Keyword	This field displays the destination port for this rule.
IP DSCP	This field indicates the value specified for IP DSCP.
Flow Label	This field indicates the value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	Displays the queue identifier to which packets matching this rule are assigned.
Mirror Interface	Displays the interface to which packets matching this rule are copied.
Redirect Interface	Displays the interface to which packets matching this rule are forwarded.

IPv6 MLD Snooping Querier Commands

This chapter explains the following commands:

- `ipv6 mld snooping querier`
- `ipv6 mld snooping querier (VLAN mode)`
- `ipv6 mld snooping querier address`
- `ipv6 mld snooping querier election participate`
- `ipv6 mld snooping querier query-interval`
- `ipv6 mld snooping querier timer expiry`
- `show ipv6 mld snooping querier`

ipv6 mld snooping querier

Use the `ipv6 mld snooping querier` command to enable MLD Snooping Querier on the system. Use the "no" form of this command to disable MLD Snooping Querier.

Syntax

`ipv6 mld snooping querier`

`no ipv6 mld snooping querier`

Default Configuration

MLD Snooping Querier is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 mld snooping querier
```

ipv6 mld snooping querier (VLAN mode)

Use the `ipv6 mld snooping querier` command in VLAN mode to enable MLD Snooping Querier on a VLAN. Use the "no" form of this command to disable MLD Snooping Querier on a VLAN.

Syntax

`ipv6 mld snooping querier vlan-id`

`no ipv6 mld snooping querier vlan-id`

- *vlan-id*— A valid VLAN ID. (Range: 1–4093)

Default Configuration

MLD Snooping Querier is disabled by default on all VLANs.

Command Mode

VLAN Database mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-vlan)#ipv6 mld snooping querier 10
```

ipv6 mld snooping querier address

Use the `ipv6 mld snooping querier address` command to set the global MLD Snooping Querier address. Use the "no" form of this command to reset the global MLD Snooping Querier address to the default.

Syntax

`ipv6 mld snooping querier address prefix[/prefix-length]`

`no ipv6 mld snooping querier address`

- *prefix* — The bits of the address to be configured.
- *prefix-length* — Designates how many of the high-order contiguous bits of the address make up the prefix.

Default Configuration

There is no global MLD Snooping Querier address configured by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 mld snooping querier address  
Fe80::5
```

ipv6 mld snooping querier election participate

Use the `ipv6 mld snooping querier election participate` command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is higher than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election then it will continue sending periodic queries. Use the "no" form of this command to disable election participation on a VLAN.

Syntax

`ipv6 mld snooping querier election participate vlan-id`

`no ipv6 mld snooping querier election participate vlan-id`

- *vlan-id*— A valid VLAN ID. (Range: 1 - 4093)

Default Configuration

Election participation is disabled by default.

Command Mode

VLAN Database mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-vlan)#ipv6 mld snooping querier  
election participate 10
```


ipv6 mld snooping querier query-interval

Use the `ipv6 mld snooping querier query-interval` command to set the MLD Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query. Use the "no" form of this command to reset the Query Interval to the default.

Syntax

`ipv6 mld snooping querier query-interval interval`

`ipv6 mld snooping querier query-interval`

- *interval*— Amount of time that the switch waits before sending another general query. (Range: 1–1800 seconds)

Default Configuration

The default query interval is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command

Example

```
console(config)#ipv6 mld snooping querier 120
```

ipv6 mld snooping querier timer expiry

Use the `ipv6 mld snooping querier timer expiry` command to set the MLD Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network. Use the "no" form of this command to reset the timer expiration period to the default.

Syntax

`ipv6 mld snooping querier timer expiry timer`

ipv6 mld snooping querier timer expiry

- *timer*— The time that the switch remains in Non-Querier mode after it has discovered that there is a multicast querier in the network. (Range: 60–300 seconds)

Default Configuration

The default timer expiration period is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 mld snooping querier timer  
expiry 222
```

show ipv6 mld snooping querier

Use the `show ipv6 mld snooping querier` command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Syntax

```
show ipv6 mld snooping querier [detail | vlan vlan-id]
```

- *vlan-id*— A valid VLAN ID. (Range: 1 - 4093)

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

When the optional argument `vlan vlan-id` is not used, the command shows the following information:

MLD Snooping Querier Mode	Indicates whether or not MLD Snooping Querier is active on the switch.
Querier Address	Shows the IP Address which will be used in the IPv6 header while sending out MLD queries.
MLD Version	Indicates the version of MLD that will be used while sending out the queries. This is defaulted to MLD v1 and it can not be changed.
Querier Query Interval	Shows the amount of time that a Snooping Querier waits before sending out a periodic general query.
Querier Expiry Interval	Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When the optional argument `vlan vlan-id` is used, the following additional information appears:

MLD Snooping Querier VLAN Mode	Indicates whether MLD Snooping Querier is active on the VLAN.
Querier Election Participate Mode	Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	Shows the IP Address which will be used in the IPv6 header while sending out MLD queries.
Operational State	Indicates whether MLD Snooping Querier is in "Querier" or "Non-Querier" state. When the switch is in Querier state it will send out periodic general queries. When in Non-Querier state it will wait for moving to Querier state and does not send out any queries.
Operational Version	Indicates the version of MLD that will be used while sending out the queries. This is defaulted to MLD v1 and it can not be changed.

When the optional argument detail is used, the command shows the global information and the information for all Querier enabled VLANs as well as the following information:

Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
MLD Version	Indicates the version of MLD.

iSCSI Optimization Commands

This chapter explains the following commands:

- `iscsi enable`
- `show iscsi`

iscsi enable

The **iscsi enable** command globally enables iSCSI awareness. To disable iSCSI awareness use the **no** form of this command.

Syntax

iscsi enable

no iscsi enable

Default Configuration

The default iSCSI optimization mode is disabled.



NOTE: Rapid Spanning Tree Protocol (RSTP) and flow-control are globally enabled by default.

Command Mode

Global Configuration mode.

User Guidelines

When iSCSI is enabled, the following actions occur:

- The MTU on all ports and port-channels is set to 9216 (jumbo frames are enabled).
- Flow control is globally enabled, if it is not already enabled.
- iSCSI LLDP monitoring starts to automatically detect Dell EqualLogic arrays.

When a Dell EqualLogic array is connected to the switch, the switch automatically detects the array and:

- Enables portfast on the EqualLogic port.
- Disables unicast storm control on the EqualLogic port.

When the **no iscsi enable** command is issued, iSCSI resources are released and the detection of Dell EqualLogic arrays by using LLDP is disabled.

Disabling iSCSI does not remove the MTU, flow control, portfast or storm control configuration applied as a result of enabling iSCSI.

Example

The following example enables iSCSI awareness.

```
console(config)#iscsi enable
```

show iscsi

The `show iscsi` command output indicates whether iSCSI optimization is enabled or disabled.

Syntax

```
show iscsi
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the iSCSI settings.

```
console#show iscsi
```

```
iSCSI enabled
```


LACP Commands

This chapter explains the following commands:

- lacp port-priority
- lacp system-priority
- lacp timeout
- show lacp ethernet
- show lacp port-channel

lacp port-priority

Use the **lacp port-priority** command in Interface Configuration mode to configure the priority value for physical ports. To reset to default priority value, use the **no** form of this command.

Syntax

lacp port-priority *value*

no lacp port-priority

- *value* — Port priority value. (Range: 1–65535)

Default Configuration

The default port priority value is 1.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the priority value for port 1/g8 to 247.

```
console(config)#interface ethernet 1/g8
```

```
console(config-if-1/g8)#lacp port-priority 247
```

lacp system-priority

Use the **lacp system-priority** command in Global Configuration mode to configure the Link Aggregation system priority. To reset to default, use the **no** form of this command.

Syntax

lacp system-priority *value*

no lacp system-priority

- *value* — Port priority value. (Range: 1–65535)

Default Configuration

The default system priority value is 1.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the system priority to 120.

```
console(config)#lacp system-priority 120
```

lacp timeout

Use the **lacp timeout** command in Interface Configuration mode to assign an administrative LACP timeout. To reset the default administrative LACP timeout, use the **no** form of this command.

Syntax

lacp timeout {long|short}

no lacp timeout

- **long** — Specifies a long timeout value.
- **short** — Specifies a short timeout value.

Default Configuration

The default port timeout value is **long**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example assigns an administrative LACP timeout for port 1/g8 to a long timeout value.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#lACP timeout long
```

show lacp ethernet

Use the **show lacp ethernet** command in Privileged EXEC mode to display LACP information for Ethernet ports.

Syntax

show lacp ethernet *interface* [**parameters** | **statistics**]

- *Interface* — Ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display LACP Ethernet interface information.

```
console#show lacp ethernet 1/g1
Port 1/g1 LACP parameters:
Actor
```

system priority:	1
system mac addr:	00:00:12:34:56:78
port Admin key:	30
port Oper key:	30
port Oper priority:	1
port Admin timeout:	LONG
port Oper timeout:	LONG
LACP Activity:	ACTIVE
Aggregation:	AGGREGATABLE
synchronization:	FALSE
collecting:	FALSE
distributing:	FALSE
expired:	FALSE

Partner

system priority:	0
system mac addr:	00:00:00:00:00:00
port Admin key:	0
port Oper key:	0
port Admin priority:	0
port Oper priority:	0
port Oper timeout:	LONG
LACP Activity:	ASSIVE
Aggregation:	AGGREGATABLE
synchronization:	FALSE
collecting:	FALSE
distributing:	FALSE

```

expired:                                FALSE
Port 1/g1 LACP Statistics:
LACP PDUs sent:                        2
LACP PDUs received:                    2

```

show lacp port-channel

Use the **show lacp port-channel** command in Privileged EXEC mode to display LACP information for a port-channel.

Syntax

show lacp port-channel [*port_channel_number*]

- *port_channel_number* — The port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display LACP port-channel information.

```

console#show lacp port-channel 1
Port-Channel 1:Port Type 1000 Ethernet
Actor
System Priority:                        1
AC Address:                            000285:0E1C00
Admin Key:                             29

```

Oper Key:	29
Partner	
System Priority:	0
MAC Address:	000000:000000
Oper Key:	14

Link Dependency Commands

This chapter explains the following commands:

- link-dependency group
- no link-dependency group
- add ethernet
- add port-channel
- add port-channel
- no add port-channel
- depends-on ethernet
- no depends-on ethernet
- depends-on port-channel
- no depends-on port-channel
- show link-dependency

link-dependency group

Use the **link-dependency group** command to enter the link-dependency mode to configure a link-dependency group

Syntax

link-dependency group *GroupId*

- *GroupId* — Link dependency group identifier. (Range: 1–16)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

No specific guidelines

Example

```
console(config)#link-dependency group 1
console(config-linkDep-group-1)#
```

no link-dependency group

Use the **no link-dependency group** command to remove the configuration for a link-dependency group.

Syntax

no link-dependency group *GroupId*

- *GroupId* — Link dependency group identifier. (Range: 1–16)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

No specific guidelines

Example

```
console(config)#no link-dependency group 1
```

add ethernet

Use the **add ethernet** command to add member Ethernet port(s) to the dependency list.

Syntax

add ethernet *intf-list*

- *intf-list* — List of Ethernet interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid Ethernet interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-depend-1)#add ethernet 1/g1
```

add port-channel

Use the **add port-channel** command to add member port-channels to the dependency list.

Syntax

add port-channel *port-channel-list*

- *port-channel-list* — List of port-channel interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid port-channel interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)#add port-channel 2
```

no add port-channel

Use the **no add port-channel** command to remove member port-channels from the dependency list.

Syntax

no add port-channel *port channel list*

- *port-channel-list* — List of port-channel interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid port-channel interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)#no add port-channel 2
```

depends-on ethernet

Use the **depends-on ethernet** command to add the dependent Ethernet ports list.

Syntax

depends-on ethernet *intf-list*

- *intf-list* — List of Ethernet interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid Ethernet interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)#depends-on ethernet  
1/g10
```

no depends-on ethernet

Use the **no depends-on ethernet** command to remove the dependent Ethernet ports list.

Syntax

no depends-on ethernet *intf-list*

- *intf-list* — List of Ethernet interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid Ethernet interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)#no depends-on  
ethernet 1/g10
```

depends-on port-channel

Use the **depends-on port-channel** command to add the dependent port-channels list.

Syntax

depends-on port-channel *port-channel-list*

- *port-channel-list* — List of port-channel interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid port-channel interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console (config-linkDep-group-1) #depends-on port-  
channel 6
```

no depends-on port-channel

Use the **no depends-on port-channel** command to remove the dependent port-channels list.

Syntax

no depends-on port-channel *port-channel-list*

- *port-channel-list* — List of port-channel interfaces. Separate nonconsecutive ports with a comma and no spaces. Use a hyphen to designate the range of ports. (Range: Valid port-channel interface list or range)

Default Configuration

This command has no default configuration.

Command Mode

Link Dependency mode

User Guidelines

No specific guidelines

Example

```
console(config-linkDep-group-1)# no depends-on port-  
channel 6
```

show link-dependency

Use the **show link-dependency** command to show the link dependencies configured for a particular group. If no group is specified, then all the configured link-dependency groups are displayed.

Syntax

```
show link-dependency [group GroupId]
```

- *GroupId* — Link dependency group identifier. (Range: Valid Group Id, 1–16)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

No specific guidelines

Example

The following command shows link dependencies for all groups.

```
console#show link-dependency
```

GroupId	Member Ports	Ports Depended On
-----	-----	-----
2	1/g1-1/g4	1/g8-1/g9
3	1/g5	ch2
5	1/g3-1/g4	1/g10

The following command shows link dependencies for group 2 only.

```
console#show link-dependency group 2
```

GroupId	Member Ports	Ports Depended On
-----	-----	-----
2	1/g1-1/g4	1/g8-1/g9

LLDP Commands

This chapter explains the following commands:

- clear lldp remote-data
- clear lldp statistics
- lldp med
- lldp med confignotification
- lldp med faststartrepeatcount
- lldp med transmit-tlv
- lldp notification
- lldp notification-interval
- lldp receive
- lldp timers
- lldp transmit
- lldp transmit-mgmt
- lldp transmit-tlv
- show lldp
- show lldp interface
- show lldp local-device
- show lldp med
- show lldp med interface
- show lldp med local-device
- show lldp med remote-device
- show lldp remote-device
- show lldp statistics

clear lldp remote-data

Use the `clear lldp remote-data` command in Privileged EXEC mode to delete all LLDP information from the remote data table.

Syntax

```
clear lldp remote-data
```

Default Configuration

By default, data is removed only on system reset.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to clear the LLDP remote data.

```
console#clear lldp remote-data
```

clear lldp statistics

Use the `clear lldp statistics` command in Privileged EXEC mode to reset all LLDP statistics.

Syntax

```
clear lldp statistics
```

Default Configuration

By default, the statistics are only cleared on a system reset.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to reset all LLDP statistics.

```
console#clear lldp statistics
```

lldp med

This command is used to enable/disable LLDP-MED on an interface. By enabling MED, the transmit and receive functions of LLDP are effectively enabled.

Syntax Description

lldp med

no lldp med

Parameter Ranges

Not applicable

Command Mode

Interface (Ethernet) Configuration

Default Value

LLDP-MED is disabled on all supported interfaces.

Usage Guidelines

No specific guidelines.

Example

```
console(config)#interface ethernet 1/g1  
console(config-if-1/g1)#lldp med
```

Ildp med confignotification

This command is used to enable sending the topology change notification.

Syntax Description

lldp med confignotification

no lldp med confignotification

Parameter Ranges

Not applicable

Command Mode

Interface (Ethernet) Configuration

Default Value

By default, notifications are disabled on all supported interfaces.

Usage Guidelines

No specific guidelines.

Example

```
console(config)#lldp med confignotification
```

Ildp med faststartrepeatcount

This command is used to set the value of the fast start repeat count.

Syntax Description

lldp med faststartrepeatcount *count*

no lldp med faststartrepeatcount

- *count*— Number of LLDP PDUs that are transmitted when the protocol is enabled. (Range 1–10)

Command Mode

Global Configuration

Default Value

3

Usage Guidelines

No specific guidelines.

Example

```
console(config)# lldp med faststartrepeatcount 2
```

Ildp med transmit-tlv

This command is used to specify which optional TLVs in the LLDP MED set are transmitted in the LLDPDUs. There are certain conditions that have to be met for this port to be MED compliant. These conditions are explained in the normative section of the specification. For example, the MED TLV 'capabilities' is mandatory. By disabling this bit, MED is effectively disable on this interface.

Syntax Description

lldp med transmit-tlv [*capabilities*] [*network-policy*] [*ex-pse*] [*ex-pd*]
[*location*] [*inventory*]

no med lldp transmit-tlv [*capabilities*] [*network-policy*] [*ex-pse*] [*ex-pd*]
[*location*] [*inventory*]

- *Capabilities* — Transmit the capabilities TLV
- *network-policy* — Transmit the network policy TLV
- *ex-pse* — Transmit the extended PSE TLV
- *ex-pd* — Transmit the extended PD TLV
- *Location* — Transmit the location TLV
- *Inventory* — Transmit the inventory TLV

Parameter Ranges

Not applicable. Command accepts keywords only.

Command Mode

Interface (Ethernet) Configuration

Default Value

By default, the capabilities and network policy TLVs are included.

Example

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#lldp med transmit-tlv
capabilities
console(config-if-1/g1)#lldp med transmit-tlv
network-policies
```

lldp notification

Use the **lldp notification** command in Interface Configuration mode to enable remote data change notifications. To disable notifications, use the **no** form of this command.

Syntax

```
lldp notification
no lldp notification
```

Default Configuration

By default, notifications are disabled on all supported interfaces.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to enable remote data change notifications.

```
console(config-if-1/g3)#lldp notification
```

lldp notification-interval

Use the **lldp notification-interval** command in Global Configuration mode to limit how frequently remote data change notifications are sent. To return the notification interval to the factory default, use the **no** form of this command.

Syntax

lldp notification-interval *interval*

no lldp notification-interval

- *interval* — The smallest interval in seconds at which to send remote data change notifications. (Range: 5–3600 seconds)

Default Configuration

The default value is 5 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to set the interval value to 10 seconds.

```
console(config)#lldp notification-interval 10
```

lldp receive

Use the **lldp receive** command in Interface Configuration mode to enable the LLDP receive capability. To disable reception of LLDPDUs, use the **no** form of this command.

Syntax

lldp receive

no lldp receive

Default Configuration

The default lldp receive mode is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to enable the LLDP receive capability.

```
console(config-if-1/g3)#lldp receive
```

lldp timers

Use the **lldp timers** command in Global Configuration mode to set the timing parameters for local data transmission on ports enabled for LLDP. To return any or all parameters to factory default, use the **no** form of this command.

Syntax

lldp timers [*interval transmit-interval*] [*hold hold-multiplier*] [*reinit reinit-delay*]

no lldp timers [*interval*] [*hold*] [*reinit*]

- *transmit-interval* — The interval in seconds at which to transmit local data LLDPDUs. (Range: 5–32768 seconds)
- *hold-multiplier* — Multiplier on the transmit interval used to set the TTL in local data LLDPDUs. (Range: 2–10)
- *reinit-delay* — The delay in seconds before re-initialization. (Range: 1–10 seconds)

Default Configuration

The default transmit interval is 30 seconds.

The default hold-multiplier is 4.

The default delay before re-initialization is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays how to configure LLDP to transmit local information every 1000 seconds.

```
console(config)#lldp timers interval 1000
```

The following example displays how to set the timing parameter at 1000 seconds with a hold multiplier of 8 and a 5 second delay before re-initialization.

```
console(config)#lldp timers interval 1000 hold 8  
reinit 5
```

lldp transmit

Use the **lldp transmit** command in Interface Configuration mode to enable the LLDP advertise (transmit) capability. To disable local data transmission, use the **no** form of this command.

Syntax

lldp transmit

no lldp transmit

Default Configuration

LLDP is disabled on all supported interfaces.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how enable the transmission of local data.

```
console(config-if-1/g3)#lldp transmit
```

lldp transmit-mgmt

Use the **lldp transmit-mgmt** command in Interface Configuration mode to include transmission of the local system management address information in the LLDPDU. To cancel inclusion of the management information, use the **no** form of this command.

Syntax

lldp transmit-mgmt

no lldp transmit-mgmt

Default Configuration

By default, management address information is not included.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to include management information in the LLDPDU.

```
console(config-if-1/g3)#lldp transmit-mgmt
```

lldp transmit-tlv

Use the **lldp transmit-tlv** command in Interface Configuration mode to specify which optional type-length-value settings (TLVs) in the 802.1AB basic management set will be transmitted in the LLDPDUs. To remove an optional TLV, use the **no** form of this command.

Syntax

```
lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]
```

```
no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]
```

- **sys-name** — Transmits the system name TLV
- **sys-desc** — Transmits the system description TLV
- **sys-cap** — Transmits the system capabilities TLV
- **port desc** — Transmits the port description TLV

Default Configuration

By default, no optional TLVs are included.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to include the system description TLV in local data transmit.

```
console(config-if-1/g3)#lldp transmit-tlv sys-desc
```

show lldp

Use the **show lldp** command in Privileged EXEC mode to display the current LLDP configuration summary.

Syntax

```
show lldp
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the current LLDP configuration summary.

```
console# show lldp
```

```
Global Configurations:
```

```
Transmit Interval: 30 seconds
```

```
Transmit TTL Value: 120 seconds
```

```
Reinit Delay: 2 seconds
```

```
Notification Interval: limited to every 5 seconds
```

```
console#show lldp
```

```
LLDP transmit and receive disabled on all interfaces
```

show lldp interface

Use the **show lldp interface** command in Privileged EXEC mode to display the current LLDP interface state.

Syntax

```
show lldp interface {interface | all}
```

- *interface* — Specifies a valid physical interface on the switch or unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

This example show how the information is displayed when you use the command with the **all** parameter.

```
console#show lldp interface all
```

Interface	Link	Transmit	Receive	Notify	TLVs	Mgmt
-----	----	-----	-----	-----	-----	----
1/g1	Up	Enabled	Enabled	Enabled	0,1,2,3	Y
1/g2	Down	Enabled	Enabled	Disabled		Y
1/g3	Down	Disabled	Disabled	Disabled	1,2	N

TLV Codes: 0 - Port Description, 1 - System Name, 2 - System Description, 3 -

System Capability

```
console# show lldp interface 1/g1
```

Interface	Link	Transmit	Receive	Notify	TLVs	Mgmt
1/g1	Up	Enabled	Enabled	Enabled	0,1,2,3	Y

TLV Codes: 0 - Port Description, 1 - System Name, 2 - System Description, 3 - System Capability

show lldp local-device

Use the `show lldp local-device` command in Privileged EXEC mode to display the advertised LLDP local data. This command can display summary information or detail for each interface.

Syntax

```
show lldp local-device {detail interface | interface | all}
```

- **detail** — includes a detailed version of remote data.
- *interface* — Specifies a valid physical interface on the device, unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

These examples show advertised LLDP local data in two levels of detail.

```
console#show lldp local-device all
```

```
LLDP Local Device Summary
```


Interface	Port ID	Port Description
1/g1	00:62:48:00:00:02	

```

console# show lldp local-device detail 1/g1
LLDP Local Device Detail
Interface: 1/g1
Chassis ID Subtype: MAC Address
Chassis ID: 00:62:48:00:00:00
Port ID Subtype: MAC Address
Port ID: 00:62:48:00:00:02
System Name:
System Description: Routing
Port Description:
System Capabilities Supported: bridge, router
System Capabilities Enabled: bridge
Management Address:
Type: IPv4
Address: 192.168.17.25

```

show lldp med

This command displays a summary of the current LLDP MED configuration.

Syntax Description

show lldp med

Parameter Ranges

Not applicable

Command Mode

Privileged EXEC

Default Value

Not applicable

Usage Guidelines

No specific guidelines.

Example

```
console(config)#show lldp med
LLDP MED Global Configuration
```

```
Fast Start Repeat Count: 3
```

```
Device Class: Network Connectivity
```

show lldp med interface

This command displays a summary of the current LLDP MED configuration for a specific interface.

Syntax Description

show lldp med interface {<unit/port> | all}

- *unit/port* — Indicates a specific physical interface.

- All — Indicates all valid LLDP interfaces.

Parameter Ranges

Not applicable

Command Mode

Privileged EXEC.

Default Value

Not applicable

Example

```
console#show lldp med interface all
```

LLDP MED Interface Configuration

Interface	Link	configMED	operMED	ConfigNotify	TLVsTx
-----	-----	-----	-----	-----	-----
1/g1	Down	Disabled	Disabled	Disabled	
1/g2	Down	Disabled	Disabled	Disabled	

```
console #show lldp med interface 1/g1
```

LLDP MED Interface Configuration

Interface	Link	configMED	operMED	ConfigNotify	TLVsTx
-----	-----	-----	-----	-----	-----
1/g1	Up	Enabled	Enabled	Disabled	0,1

TLV Codes: 0- Capabilities, 1- Network Policy
2-Location, 3- Extended PSE, 4- Extended PD, 5-Inventory

show lldp med local-device

This command displays the advertised LLDP local data. This command can display summary information or detail for each interface.

Syntax Description

`show lldp med local-device detail <unit/port>`

- *unit/port* — Indicates a specific physical interface.
- **detail** — Includes a detailed version of remote data for the indicated interface.

Parameter Ranges

Not applicable

Command Mode

Privileged EXEC

Default Value

Not applicable

Example

```
Console#show lldp med local-device detail 1/g1
```

```
LLDP MED Local Device Detail
```

```
Interface: 1/0/8
```

```
Network Policies
```

```
Media Policy Application Type : voice
```

```
Vlan ID: 10
```

```
Priority: 5
```

DSCP: 1

Unknown: False

Tagged: True

Media Policy Application Type : streamingvideo

Vlan ID: 20

Priority: 1

DSCP: 2

Unknown: False

Tagged: True

Inventory

Hardware Rev: xxx xxx xxx

Firmware Rev: xxx xxx xxx

Software Rev: xxx xxx xxx

Serial Num: xxx xxx xxx

Mfg Name: xxx xxx xxx

Model Name: xxx xxx xxx

Asset ID: xxx xxx xxx

Location

Subtype: elin

Info: xxx xxx xxx

Extended POE

Device Type: pseDevice

Extended POE PSE

Available: 0.3 watts

Source: primary

Priority: critical

Extended POE PD

Required: 0.2 watts

Source: local

Priority: low

show lldp med remote-device

This command displays the current LLDP MED remote data. This command can display summary information or detail for each interface.

Syntax Description

`show lldp med remote-device { <unit/port> | all }`

`show lldp med remote-device detail <unit/port>`

- *unit/port* — Indicates a specific physical interface.
- **all** — Indicates all valid LLDP interfaces.
- **detail** — Includes a detailed version of remote data for the indicated interface.

Parameter Ranges

Not applicable

Command Mode

Privileged EXEC

Default Value

Not applicable

Example

```
Console#show lldp med remote-device all
```

```
LLDP MED Remote Device Summary
```

```
Local
```

```
InterfaceDevice Class
```

```
-----
```

```
1/g1Class I
```

```
1/g2 Not Defined
```

```
1/g3Class II
```

```
1/g4Class III
```

```
1/g5Network Con
```

```
Console#show lldp med remote-device detail 1/g1
```

```
LLDP MED Remote Device Detail
```

```
Local Interface: 1/g1
```

```
Capabilities
```

```
MED Capabilities Supported: capabilities,  
networkpolicy, location, extendedpse
```

```
MED Capabilities Enabled: capabilities, networkpolicy
```

```
Device Class: Endpoint Class I
```

Network Policies

Media Policy Application Type : voice

Vlan ID: 10

Priority: 5

DSCP: 1

Unknown: False

Tagged: True

Media Policy Application Type : streamingvideo

Vlan ID: 20

Priority: 1

DSCP: 2

Unknown: False

Tagged: True

Inventory

Hardware Rev: xxx xxx xxx

Firmware Rev: xxx xxx xxx

Software Rev: xxx xxx xxx

Serial Num: xxx xxx xxx

Mfg Name: xxx xxx xxx

Model Name: xxx xxx xxx

Asset ID: xxx xxx xxx

Location

Subtype: elin

Info: xxx xxx xxx

Extended POE

Device Type: pseDevice

Extended POE PSE

Available: 0.3 Watts

Source: primary

Priority: critical

Extended POE PD

Required: 0.2 Watts

Source: local

Priority: low

show lldp remote-device

Use the **lldp remote-device** command in Privileged EXEC mode to display the current LLDP remote data. This command can display summary information or detail for each interface.

Syntax

show lldp remote-device {**detail** *interface* | *interface* | **all**}

- **detail** — Includes detailed version of remote data.
- *interface* — Specifies a valid physical interface on the device, unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

These examples show current LLDP remote data, including a detailed version.

```
console#show lldp remote-device
```

Local Remote			
Interface	Device	ID Port	ID TTL
-----	-----	-----	-----
1/g1	01:23:45:67:89:AB	01:23:45:67:89:AC	60 seconds
1/g2	01:23:45:67:89:CD	01:23:45:67:89:CE	120 seconds
1/g3	01:23:45:67:89:EF	01:23:45:67:89:FG	80 seconds

```
console# show lldp remote-device detail 1/g1
```

```
Ethernet1/g1,  
Remote ID: 01:23:45:67:89:AB  
System Name: system-1  
System Description:  
System Capabilities: Bridge  
Port ID: 01:23:45:67:89:AC  
Port Description: 1/g4  
Management Address: 192.168.112.1  
TTL: 60 seconds
```

show lldp statistics

Use the **show lldp statistics** command in Privileged EXEC mode to display the current LLDP traffic statistics.

Syntax

show lldp statistics {*interface* | **all**}

- *interface* — Specifies a valid physical interface on the switch or unit/port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples shows an example of the display of current LLDP traffic statistics.

```
console#show lldp statistics all
```

```
LLDP Device Statistics
```

```
Last Update..... 0 days 22:58:29
```

```
Total Inserts..... 1
```

```
Total Deletes..... 0
```

```
Total Drops..... 0
```

```

Total Ageouts..... 1

      Tx      Rx      TLV      TLV      TLV
TLV  TLV
Interface Total Total Discards Errors Ageout Discards Unknowns MED
802.1 802.3
-----
1/g11      29395 82562 0          0      1      0          0          0      1
4

```

The following table explains the fields in this example.

Parameter	Description
Last Update	The value of system of time the last time a remote data entry was created, modified, or deleted.
Total Inserts	The number of times a complete set of information advertised by a remote device has been inserted into the table.
Total Deletes	The number of times a complete set of information advertised by a remote device has been deleted from the table.
Total Drops	Number of times a complete set of information advertised by a remote device could not be inserted due to insufficient resources.
Total Ageouts	Number of times any remote data entry has been deleted due to time-to-live (TTL) expiration.
Transmit Total	Total number of LLDP frames transmitted on the indicated port.
Receive Total	Total number of valid LLDP frames received on the indicated port.
Discards	Number of LLDP frames received on the indicated port and discarded for any reason.

Parameter	Description
Errors	Number of non-valid LLDP frames received on the indicated port.
Ageouts	Number of times a remote data entry on the indicated port has been deleted due to TTL expiration.
TLV Discards	Number LLDP TLVs (Type, Length, Value sets) received on the indicated port and discarded for any reason by the LLDP agent.
TLV Unknowns	Number of LLDP TLVs received on the indicated port for a type not recognized by the LLDP agent.
TLV MED	Number of OUI specific MED (Media Endpoint Device) TLVs received.
TLV 802.1	Number of OUI specific 802.1 specific TLVs received.
TLV 802.3	Number of OUI specific 802.3 specific TLVs received.

Port Channel Commands

This chapter explains the following commands:

- `channel-group`
- `interface port-channel`
- `interface range port-channel`
- `hashing-mode`
- `no hashing-mode`
- `show interfaces port-channel`
- `show statistics port-channel`

channel-group

Use the **channel-group** command in Interface Configuration mode to configure a port-to-port channel. To remove the channel-group configuration from the interface, use the **no** form of this command.

Syntax

channel-group *port-channel-number* **mode** {**on** | **auto**}

no channel-group

- *port-channel-number* — Number of a valid port-channel for the current port to join.
- **on** — Forces the port to join a channel without LACP.
- **auto** — Forces the port to join a channel with LACP.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how port 1/g5 is configured to port-channel number 1 without LACP.

```
console(config)# interface ethernet 1/g5
```

```
console(config-if-1/g5)# channel-group 1 mode on
```


interface port-channel

Use the **interface port-channel** command in Global Configuration mode to configure a port-channel type and enter port-channel configuration mode.

Syntax

interface port-channel *port-channel-number*

- *port-channel-number* — A valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters the context of port-channel number 1.

```
console(config)# interface port-channel 1
console(config-if-ch1)#
```

interface range port-channel

Use the **interface range port-channel** command in Global Configuration mode to execute a command on multiple port channels at the same time.

Syntax

interface range port-channel {*port-channel-range*/**all**}

- *port-channel-range* — List of port-channels to configure. Separate non-consecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels. (Range: valid port-channel)
- **all** — All the channel-ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands in the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, it stops the execution of the command on subsequent interfaces.

Example

The following example shows how port-channels 1, 2 and 8 are grouped to receive the same command.

```
console(config)# interface range port-channel 1-2,8
console(config-if)#
```

hashing-mode

Use the **hashing-mode** command to set the hashing algorithm on trunk ports.

Syntax

hashing-mode *mode*

- *mode* — Mode value in the range of 1 to 6.

Range: 1–6:

- 1 — Source MAC, VLAN, EtherType, source module, and port ID
- 2 — Destination MAC, VLAN, EtherType, source module, and port ID
- 3 — Source IP and source TCP/UDP port
- 4 — Destination IP and destination TCP/UDP port
- 5 — Source/destination MAC, VLAN, EtherType, and source MODID/port
- 6 — Source/destination IP and source/destination TCP/UDP port

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (port-channel)

User Guidelines

No specific guidelines.

Example

```
console(config)#interface port-channel 1
console(config-if-ch1)#hashing-mode 4
```

no hashing-mode

Use the **no hashing-mode** command to set the hashing algorithm on Trunk ports to the default (3).

Syntax Description

no hashing-mode

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (port-channel)

User Guidelines

No specific guidelines.

Example

```
console(config)#interface port-channel 1
console(config-if-ch1)#no hashing mode
```

show interfaces port-channel

Use the `show interfaces port-channel` command to show port-channel information.

Syntax Description

`show interfaces port-channel` [*port-channel number*]

- [*port-channel-number*] — Number of the port channel to show. This parameter is optional. If the port channel number is not given, all the channel groups are displayed. (Range: Valid port-channel number, 1 to 48)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

No specific guidelines.

Example

Console#show interfaces port-channel

Channel	Ports	Hashing-mode
-----	-----	-----
ch1	Active: 1/e1, 2/e2	1
ch2	Active: 2/e2, 2/e7 Inactive: 3/e1	2
ch3	Active: 3/e3, 3/e8	3 <default>
ch4	No Configured Ports	5
ch5	No Configured Ports	6
ch6	No Configured Ports	4
ch7	No Configured Ports	3 <default>
ch8	No Configured Ports	3 <default>

Hash algorithm type

- 1 - Source MAC, VLAN, EtherType, source module and port Id
- 2 - Destination MAC, VLAN, EtherType, source module and port Id
- 3 - Source IP and source TCP/UDP port
- 4 - Destination IP and destination TCP/UDP port
- 5 - Source/Destination MAC, VLAN, EtherType and source MODID/port
- 6 - Source/Destination IP and source/destination TCP/UDP port

show statistics port-channel

Use the **show statistics port-channel** command in Privileged EXEC mode to display statistics about a specific port-channel.

Syntax

show statistics port-channel *port-channel-number*

- *port-channel-number* — Valid port-channel number channel to display.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows statistics about port-channel 1.

```
console#show statistics port-channel 1
```

```

Total Packets Received (Octets)..... 0
Packets Received > 1522 Octets..... 0
Packets RX and TX 64 Octets..... 1064
Packets RX and TX 65-127 Octets..... 140
Packets RX and TX 128-255 Octets..... 201
Packets RX and TX 256-511 Octets..... 418
Packets RX and TX 512-1023 Octets..... 1
Packets RX and TX 1024-1518 Octets..... 0
Packets RX and TX 1519-1522 Octets..... 0
Packets RX and TX 1523-2047 Octets..... 0
Packets RX and TX 2048-4095 Octets..... 0
Packets RX and TX 4096-9216 Octets..... 0
Total Packets Received Without Errors..... 0
Unicast Packets Received..... 0
Multicast Packets Received..... 0
Broadcast Packets Received..... 0
Total Packets Received with MAC Errors..... 0
Jabbers Received..... 0
Fragments/Undersize Received..... 0
Alignment Errors..... 0
--More-- or (q)uit
FCS Errors..... 0
Overruns..... 0
Total Received Packets Not Forwarded..... 0
Local Traffic Frames..... 0
802.3x Pause Frames Received..... 0

```

```

Unacceptable Frame Type..... 0
Multicast Tree Viable Discards..... 0
Reserved Address Discards..... 0
Broadcast Storm Recovery..... 0
CFI Discards..... 0
Upstream Threshold..... 0
Total Packets Transmitted (Octets).....
263567
Max Frame Size..... 1518
Total Packets Transmitted Successfully..... 1824
Unicast Packets Transmitted..... 330
Multicast Packets Transmitted..... 737
Broadcast Packets Transmitted..... 757
Total Transmit Errors..... 0
FCS Errors..... 0
--More-- or (q)uit
Tx Oversized..... 0
Underrun Errors..... 0
Total Transmit Packets Discarded..... 0
Single Collision Frames..... 0
Multiple Collision Frames..... 0
Excessive Collision Frames..... 0
Port Membership Discards..... 0
802.3x Pause Frames Transmitted..... 0
GVRP PDUs received..... 0
GVRP PDUs Transmitted..... 0

```

```
GVRP Failed Registrations..... 0
Time Since Counters Last Cleared..... 0 day
0 hr 17 min 52 sec
console#
```


Port Monitor Commands

This chapter explains the following commands:

- monitor session
- show monitor session

monitor session

Use the **monitor session** command in Global Configuration mode to configure a probe port and a monitored port for monitor session (port monitoring). Use the **src-interface** parameter to specify the interface to monitor. Use **rx** to monitor only ingress packets, or use **tx** to monitor only egress packets. If you do not specify an {**rx** | **tx**} option, the destination port monitors both ingress and egress packets. Use the destination interface to specify the interface to receive the monitored traffic. Use the **mode** parameter to enable the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Syntax

monitor session *session-id* {**source interface** *src-interface* [**rx** | **tx**] | **destination interface** *dst-interface* | **mode**}

no monitor session

- *session id* — Session identification number.
- **src-interface** — Ethernet interface (Range: Any valid Ethernet Port)
- **rx** — Monitors received packets only. If no option specified, monitors both rx and tx
- **tx** — Monitors transmitted packets only. If no option is specified, monitors both rx and tx.
- **dst-interface** — Ethernet interface (Range: Any valid Ethernet Port)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following examples shows various port monitoring configurations.

```
console(config)#monitor session 1 source interface
1/g8

console(config)#monitor session 1 destination
interface 1/g10

console(config)#monitor session 1 mode
```

show monitor session

Use the **show monitor session** command in Privileged EXEC mode to display status of port monitoring.

Syntax

```
show monitor session session-id
```

- session id*— Session identification number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples shows port monitoring status.

```
console#show monitor session 1
```

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
-----	-----	-----	-----	-----
1	Enable	1/g10	1/g8	Rx, Tx

QoS Commands

This chapter explains the following commands:

- `assign-queue`
- `class`
- `class-map`
- `class-map rename`
- `classofservice dot1p-mapping`
- `classofservice ip-dscp-mapping`
- `classofservice trust`
- `conform-color`
- `cos-queue min-bandwidth`
- `cos-queue strict`
- `diffserv`
- `drop`
- `mark cos`
- `mark ip-dscp`
- `mark ip-precedence`
- `match class-map`
- `match cos`
- `match destination-address mac`
- `match dstip`
- `match dstip6`
- `match dstl4port`
- `match ethertype`
- `match ip6flowlbl`
- `match ip dscp`
- `match ip precedence`

- match ip tos
- match protocol
- match source-address mac
- match srcip
- match srcip6
- match srcl4port
- match vlan
- mirror
- police-simple
- policy-map
- redirect
- service-policy
- show class-map
- show classofservice dot1p-mapping
- show classofservice ip-dscp-mapping
- show classofservice trust
- show diffserv
- show diffserv service interface ethernet in
- show diffserv service interface port-channel in
- show diffserv service brief
- show interfaces cos-queue
- show policy-map
- show policy-map interface
- show service-policy
- traffic-shape

assign-queue

Use the **assign-queue** command in Policy-Class-Map Configuration mode to modify the queue ID to which the associated traffic stream is assigned.

Syntax

assign-queue <*queueid*>

- *queueid* — Specifies a valid queue ID. (Range: integer from 0–6.)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to change the queue ID to 4 for the associated traffic stream.

```
console (config-policy-classmap) #assign-queue 4
```

class

Use the **class** command in Policy-Map Class Configuration mode to create an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements.

Syntax

class *classname*

no class

- *classname* — Specifies the name of an existing DiffServ class. (Range: 1–31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Policy Map Configuration mode

User Guidelines

This command causes the specified policy to create a reference to the class definition. The command mode is changed to Policy-Class-Map Configuration when this command is executed successfully.

Example

The following example shows how to specify the DiffServ class name of "DELL."

```
console(config)#policy-map DELL1
console(config-classmap)#class DELL
```

class-map

Use the **class-map** command in Global Configuration mode to define a new DiffServ class of type *match-all*. To delete the existing class, use the **no** form of this command.

Syntax

class-map match-all *class-map-name* [{**ipv4** | **ipv6**}]

no class-map match-all *class-map-name*

- *class-map-name* — a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

Default Configuration

The class-map defaults to ipv4.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example creates a class-map named "DELL" which requires all ACE's to be matched.

```
console (config) #class-map DELL
console (config-cmap) #
```

class-map rename

Use the **class-map rename** command in Global Configuration mode to change the name of a DiffServ class.

Syntax

class-map rename <classname> <newclassname>

- *classname* — The name of an existing DiffServ class. (Range: 1–31 characters)
- *newclassname* — A case-sensitive alphanumeric string. (Range: 1–31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to change the name of a DiffServ class from "DELL" to "DELL1."

```
console (config) #class-map rename DELL DELL1
```

```
console (config) #
```

classofservice dot1p-mapping

Use the **classofservice dot1p-mapping** command in Global Configuration mode to map an 802.1p priority to an internal traffic class. In Interface Configuration mode, the mapping is applied only to packets received on that interface. Use the **no** form of the command to remove mapping between an 802.1p priority and an internal traffic class.

Syntax

```
classofservice dot1p-mapping 802.1ppriority trafficclass
```

```
no classofservice dot1p-mapping
```

- *802.1ppriority*— Specifies the user priority mapped to the specified traffic class for this switch. (Range: 0–7)
- *trafficclass*— Specifies the traffic class for this switch. (Range: 0–6)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration or Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

None

Example

The following example configures mapping for user priority 1 and traffic class 2.

```
console (config) #classofservice dot1p-mapping 1 2
```

classofservice ip-dscp-mapping

Use the **classofservice ip-dscp-mapping** command in Global Configuration mode to map an IP DSCP value to an internal traffic class.

Syntax

classofservice ip-dscp-mapping *ipdscp trafficclass*

- *ipdscp* — Specifies the IP DSCP value to which you map the specified traffic class. (Range: 0–63 or an IP DSCP keyword – af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef)
- *trafficclass* — Specifies the traffic class for this value mapping. (Range: 0–6)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays mapping for IP DSCP 1 and traffic class 2.

```
console(config)#classofservice ip-dscp-mapping 1 2
```

classofservice trust

Use the **classofservice trust** command in either Global Configuration mode or Interface Configuration mode to set the class of service trust mode of an interface. To set the interface mode to untrusted, use the **no** form of this command.

Syntax

classofservice trust {dot1p|untrusted|ip-dscp}

no classofservice trust

- **dot1p** — Sets the CoS mode to trust dot1p (802.1p) packet markings.
- **untrusted** — Sets the CoS Mode for all interfaces to Untrusted.
- **ip-dscp** — Specifies that the mode be set to trust IP DSCP packet markings.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode or Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays how you set the class of service trust mode of an interface to trust dot1p (802.1p) packet markings when in Global Configuration mode.

```
console(config)#classofservice trust dot1p
```

The following example displays how you set the class of service trust mode of an interface to trust IP Precedence packet mark

```
console(config)#classofservice trust ip-precedence
```

conform-color

Use the **conform-color** command in Policy-Class-Map Configuration mode to specify second-level matching for traffic flow, the only possible actions are drop, setdscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the policy command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command.

Syntax

conform-color

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to specify the **conform-color** command.

```
console (config-policy-classmap) #conform-color  
test_class (test_class is <class-map-name>
```

cos-queue min-bandwidth

Use the **cos-queue min-bandwidth** command in either Global Configuration mode or Interface Configuration mode to specify the minimum transmission bandwidth for each interface queue. To restore the default for each queue's minimum bandwidth value, use the **no** form of this command.

Syntax

cos-queue min-bandwidth *bw-0 bw-1 ... bw-n*

no cos-queue min-bandwidth

- *bw-0* — Specifies the minimum transmission bandwidth for an interface. You can specify as many bandwidths as there are interfaces (bw-0 through bw-n). (Range: 0–100 in increments of 5)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode or Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The maximum number of queues supported per interface is seven.

Example

The following example displays how to specify the minimum transmission bandwidth for seven interfaces.

```
console(config)#cos-queue min-bandwidth 0 0 5 5 10 10
10
```

cos-queue strict

Use the **cos-queue strict** command in either Global Configuration mode or Interface Configuration mode to activate the strict priority scheduler mode for each specified queue. To restore the default weighted scheduler mode for each specified queue, use the **no** form of this command.

Syntax

```
cos-queue strict {queue-id-1} [{queue-id-2} ... {queue-id-n}]
```

```
no cos-queue strict {queue-id-1} [{queue-id-2} ... {queue-id-n}]
```

- **queue-id-1** — Specifies the queue ID for which you are activating the strict priority scheduler. You can specify a queue ID for as many queues as you have (queue-id 1 through queue-id-n). (Range: 0–6)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode or Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to activate the strict priority scheduler mode for two queues.

```
console(config)#cos-queue strict 1 2
```

The following example displays how to activate the strict priority scheduler mode for three queues.

```
console(config)#cos-queue strict 1 2 4
```

diffserv

Use the **diffserv** command in Global Configuration mode to set the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated. To set the DiffServ operational mode to inactive, use the **no** form of this command.

Syntax

diffserv

no diffserv

Default Configuration

This command default is **enabled**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to set the DiffServ operational mode to active.

```
console (Config) #diffserv
```

drop

Use the **drop** command in Policy-Class-Map Configuration mode to specify that all packets for the associated traffic stream are to be dropped at ingress.

Syntax

drop

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to specify that matching packets are to be dropped at ingress.

```
console (config-policy-classmap) #drop
```


mark cos

Use the **mark cos** command in Policy-Class-Map Configuration mode to mark all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted.

Syntax

mark cos *cos-value*

- *cos-value* — Specifies the CoS value as an integer. (Range: 0–7)

Default Configuration

The default value for this command is 1.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to mark all packets with a CoS value.

```
console(config-policy-classmap)#mark cos 7
```

mark ip-dscp

Use the **mark ip-dscp** command in Policy-Class-Map Configuration mode to mark all packets for the associated traffic stream with the specified IP DSCP value.

Syntax

mark ip-dscp *dscpval*

- *dscpval*— Specifies a DSCP value (10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38, 0, 8, 16, 24, 32, 40, 48, 56, 46) or a DSCP keyword (af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef).

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to mark all packets with an IP DSCP value of "cs4."

```
console (config-policy-classmap) #mark ip-dscp cs4
```

mark ip-precedence

Use the **mark ip-precedence** command in Policy-Class-Map Configuration mode to mark all packets for the associated traffic stream with the specified IP precedence value.

Syntax

mark ip-precedence *prec-value*

- *prec-value* — Specifies the IP precedence value as an integer. (Range: 0–7)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines.

This command has no user guidelines.

Example

The following example displays

```
console(config)#policy-map p1 in
console(config-policy-map)#class c1
console(config-policy-classmap)#mark ip-precedence 2
console(config-policy-classmap)#
```

match class-map

Use the **match class-map** command to add to the specified class definition the set of match conditions defined for another class. Use the **no** form of this command to remove from the specified class definition the set of match conditions defined for another class.

Syntax

match class-map *refclassname*

no match class-map *refclassname*

- *refclassname* — The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

- The parameters *refclassname* and *class-map-name* can not be the same.
- Only one other class may be referenced by a class.

- Any attempts to delete the *refclassname* class while the class is still referenced by any *class-map-name* fails.
- The combined match criteria of *class-map-name* and *refclassname* must be an allowed combination based on the class type.
- Any subsequent changes to the *refclassname* class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

Example

The following example adds match conditions defined for the Dell class to the class currently being configured.

```
console(config-classmap)#match class-map Dell
```

The following example deletes the match conditions defined for the Dell class from the class currently being configured.

```
console(config-classmap)#no match class-map Dell
```

match cos

Use the **match cos** command in Class-Map Configuration mode to add to the specified class definition a match condition for the class of service value (the only tag in a single-tagged packet or the first or outer 802.1Q tag of a double-VLAN tagged packet).

Syntax

match cos

- **cos-value** — Specifies the CoS value as an integer (Range: 0–7)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition to the specified class.

```
console(config-classmap)#match cos 1
```

match destination-address mac

Use the **match destination-address mac** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the destination MAC address of a packet.

Syntax

match destination-address mac *macaddr macmask*

- *macaddr*— Specifies any valid layer 2 MAC address formatted as six two-digit hexadecimal numbers separated by colons.
- *macmask*— Specifies a valid layer 2 MAC address bit mask formatted as six two-digit hexadecimal numbers separated by colons. This address bit mask does not need to be contiguous.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition for the specified MAC address and bit mask.

```
console(config-classmap)#match destination-address  
mac AA:ED:DB:21:11:06 FF:FF:FF:EF:EE:EE
```

match dstip

Use the **match dstip** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the destination IP address of a packet.

Syntax

match dstip *ipaddr ipmask*

- *ipaddr* — Specifies a valid IP address.
- *ipmask* — Specifies a valid IP address bit mask. Note that even though this parameter is similar to a standard subnet mask, it does not need to be contiguous.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition using the specified IP address and bit mask.

```
console(config-classmap)#match dstip 10.240.1.1  
10.240.0.0
```

match dstip6

The **match dstip6** command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

Syntax

match dstip6 *destination-ipv6-prefix/prefix-length*

- *destination-ipv6-prefix*—IPv6 prefix in IPv6 global address format.
- *prefix-length*—IPv6 prefix length value.

Default Configuration

There is no default configuration for this command.

Command Mode

Ipv6-Class-Map Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-classmap)#match dstip6 2001:DB8::/32
```

match dstl4port

Use the **match dstl4port** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or a numeric notation.

Syntax

match dstl4port {*portkey*|*port-number*}

- *portkey*—Specifies one of the supported port name keywords. A match condition is specified by one layer 4 port number. The currently supported values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www.
- *port-number*—Specifies a layer 4 port number (Range: 0–65535).

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition based on the destination layer 4 port of a packet using the "echo" port name keyword.

```
console(config-classmap)#match dstl4port echo
```

match ethertype

Use the **match ethertype** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the ethertype.

Syntax

```
match ethertype {keyword | <0x0600-0xffff>}
```

- **keyword** — Specifies either a valid keyword or a valid hexadecimal number. The supported keywords are **appletalk**, **arp**, **ibmsna**, **ipv4**, **ipv6**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, **rarp**. (Range: 0x0600–0xFFFF)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add a match condition based on ethertype.

```
console(config-classmap)#match ethertype arp
```

match ip6flowlbl

The **match ip6flowlbl** command adds to the specified class definition a match condition based on the IPv6 flow label of a packet.

Syntax

match ip6flowlbl *label*

- *label* - The value to match in the Flow Label field of the IPv6 header (Range 0-1048575).

Default Configuration

There is no default configuration for this command.

Command Mode

Ipv6-Class-Map Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example adds a rule to match packets whose IPv6 Flow Label equals 32312.

```
console(config-classmap)#match ip6flowlbl 32312
```

match ip dscp

Use the **match ip dscp** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet. This field is defined as the high-order six bits of the Service Type octet in the IP header. The low-order two bits are not checked.

Syntax

match ip dscp *dscpval*

- *dscpval* — Specifies an integer value or a keyword value for the DSCP field. (Integer Range: 0–63) (Keyword Values: *af11*, *af12*, *af13*, *af21*, *af22*, *af23*, *af31*, *af32*, *af33*, *af41*, *af42*, *af43*, *be*, *cs0*, *cs1*, *cs2*, *cs3*, *cs4*, *cs5*, *cs6*, *cs7*, *ef*)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

The **ip dscp**, **ip precedence**, and **ip tos** match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header but with a slightly different user notation.

To specify a match on all DSCP values, use the **match ip tos** *tosbits tosmask* command with *tosbits* set to "0" (zero) and *tosmask* set to hex "03."

Example

The following example displays how to add a match condition based on the DSCP field.

```
console(config-classmap)# match ip dscp 3
```

match ip precedence

Use the **match ip precedence** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP precedence field.

Syntax

match ip precedence *precedence*

- *precedence* — Specifies the precedence field in a packet. This field is the high-order three bits of the Service Type octet in the IP header. (Integer Range: 0–7)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

The **ip dscp**, **ip precedence**, and **ip tos** match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header but with a slightly different user notation.

To specify a match on all precedence values, use the **match ip tos tosbits tosmask** command with tosbits set to "0" (zero) and tosmask set to hex "1F."

Example

The following example displays adding a match condition based on the value of the IP precedence field.

```
console(config-classmap)#match ip precedence 1
```

match ip tos

Use the **match ip tos** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP TOS field in a packet. This field is defined as all eight bits of the Service Type octet in the IP header.

Syntax

match ip tos *tosbits tosmask*

- *tosbits* — Specifies a two-digit hexadecimal number. (Range: 00–ff)
- *tosmask* — Specifies the bit positions in the *tosbits* parameter that are used for comparison against the IP TOS field in a packet. This value of this parameter is expressed as a two-digit hexadecimal number. (Range: 00–ff)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

The **ip dscp**, **ip precedence**, and **ip tos** match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header but with a slightly different user notation.

This specification is the *free form* version of the IP DSCP/Precedence/TOS match specification in that you have complete control of specifying which bits of the IP Service Type field are checked.

Example

The following example displays adding a match condition based on the value of the IP TOS field in a packet.

```
console(config-classmap)#match ip tos AA EF
```

match protocol

Use the **match protocol** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

Syntax

match protocol {*protocol-name*|*protocol-number*}

- *protocol-name* — Specifies one of the supported protocol name keywords. The supported values are *icmp*, *igmp*, *ip*, *tcp*, and *udp*.
- *protocol-number* — Specifies the standard value assigned by IANA. (Range 0–255)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition based on the "ip" protocol name keyword.

```
console(config-classmap)#match protocol ip
```

match source-address mac

Use the **match source-address mac** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the source MAC address of the packet.

Syntax

match source-address mac *address macmask*

- *macaddr* — Specifies any valid layer 2 MAC address formatted as six two-digit hexadecimal numbers separated by colons.
- *macmask* — Specifies a layer 2 MAC address bit mask formatted as six two-digit hexadecimal numbers separated by colons. This bit mask does not need to be contiguous.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example adds to the specified class definition a match condition based on the source MAC address of the packet.

```
console(config-classmap)# match source-address mac  
10:10:10:10:10:10 11:11:11:11:11:11
```

match srcip

Use the **match srcip** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the source IP address of a packet.

Syntax

match srcip *ipaddr ipmask*

- *ipaddr* — Specifies a valid IP address.
- *ipmask* — Specifies a valid IP address bit mask. Note that although this IP address bit mask is similar to a subnet mask, it does not need to be contiguous.

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition for the specified IP address and address bit mask.

```
console(config-classmap)#match srcip 10.240.1.1  
10.240.0.0
```

match srcip6

The **match srcip6** command adds to the specified class definition a match condition based on the source IPv6 address of a packet.

Syntax

match srcip6 *source-ipv6-prefix/prefix-length*

- *source-ipv6-prefix*—IPv6 prefix in IPv6 global address format.
- *prefix-length*—IPv6 prefix length value.

Default Configuration

There is no default configuration for this command.

Command Mode

Ipv6-Class-Map Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-classmap)#match srcip6 2001:DB8::/32
```

match src14port

Use the **match src14port** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or a numeric notation.

Syntax

match src14port {*portkey*|*port-number*}

- *portkey* — Specifies one of the supported port name keywords. A match condition is specified by one layer 4 port number. The currently supported values are: domain, echo, ftp, ftpdata, http, smtp,snmp, telnet, tftp, and www.
- *port-number* — Specifies a layer 4 port number (Range: 0–65535).

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add a match condition using the "snmp" port name keyword.

```
console(config-classmap)#match src14port snmp
```


match vlan

Use the **match vlan** command in Class-Map Configuration mode to add to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field. This field is the only tag in a single tagged packet or the first or outer tag of a double VLAN packet.

Syntax

match vlan <*vlan-id*>

- *vlan-id* — Specifies a VLAN ID as an integer. (Range: 0–4095)

Default Configuration

This command has no default configuration.

Command Mode

Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays adding a match condition for the VLAN ID "2."

```
console(config-classmap)#match vlan 2
```

mirror

Use the **mirror** command in Policy-Class-Map Configuration mode to mirror all the data that matches the class defined to the destination port specified.

Syntax

mirror *interface*

- *interface* — Specifies the Ethernet port to which data needs to be copied.

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

The port identified in this command is identical to the destination port of the **monitor** command.

Example

The following example displays how to copy all the data to ethernet port 1/g5.

```
console (config-policy-classmap) #mirror 1/g5
```

police-simple

Use the **police-simple** command in Policy-Class-Map Configuration mode to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and nonconform.

Syntax

```
police-simple {<datarate> <burstsize> conform-action {drop | set-  
prec-transmit <cos> | set-dscp-transmit <dscpval> | transmit}  
[violateaction {drop | set-cos-transmit <cos> | set-prec-transmit <cos> |  
set-dscp-transmit <dscpval> | transmit}]}
```

- *datarate* — Data rate in kilobits per second (kbps). (Range: 1–4294967295)
- *burstsize* — Burst size in Kbps (Range: 1–128)
- **conform action** — Indicates what happens when the packet is conforming to the policing rule: it could be dropped, it could have its COS modified, it could have its IP precedence modified, or it could have its DSCP modified. The same actions are available for packets that do not conform to the policing rule.
- *cos* — Class of Service value. (Range: 0–7)

- `dscpval` — DSCP value. (Range: 0–63 or a keyword from this list, `af11`, `af12`, `af13`, `af21`, `af22`, `af23`, `af31`, `af32`, `af33`, `af41`, `af42`, `af43`, `be`, `cs0`, `cs1`, `cs2`, `cs3`, `cs4`, `cs5`, `cs6`, `cs7`, `ef`)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

Only one style of police command (`simple`) is allowed for a given class instance in a particular policy.

Example

The following example shows how to establish the traffic policing style for the specified class.

```
console(config-policy-classmap)#police-simple 33 34
conform-action transmit violate-action transmit
```

policy-map

Use the **policy-map** command in Global Configuration mode to establish a new DiffServ policy. To remove the policy, use the **no** form of this command.

Syntax

policy-map *polycyname* [**in**]

no policy-map *polycyname*

- *polycyname* — Specifies the DiffServ policy name as a unique case-sensitive alphanumeric string of characters. (Range: 1–31 alphanumeric characters.)
- **in** — Inbound direction. Must be specified for new DiffServ policies. Not specified for existing DiffServ policies. A new policy can be specified with "in" only. An existing policy can be entered without "in" only.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The CLI mode is changed to Policy-Class-Map Configuration when this command is successfully executed.

The policy type dictates which of the individual policy attribute commands are valid within the policy definition.

Example

The following example shows how to establish a new DiffServ policy named "DELL."

```
console(config)#policy-map DELL
console(config-policy-classmap)#
```

redirect

Use the **redirect** command in Policy-Class-Map Configuration mode to specify that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Syntax

redirect *interface*

- *interface* — Specifies any valid interface. Interface is Ethernet port or port-channel (Range: lag1–lag18)

Default Configuration

This command has no default configuration.

Command Mode

Policy-Class-Map Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to redirect incoming packets to port 1/g1.

```
console (config-policy-classmap) #redirect 1/g1
```

service-policy

Use the **service-policy** command in either Global Configuration mode (for all system interfaces) or Interface Configuration mode (for a specific interface) to attach a policy to an interface. To return to the system default, use the **no** form of this command.

Syntax

service-policy in *polycymapname*

no service-policy in *polycymapname*

- *polycymapname* — Specifies the DiffServ policy name as a unique case-sensitive alphanumeric string. (Range: 1–31 alphanumeric characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode (for all system interfaces)

Interface Configuration (Ethernet, Port-channel) mode (for a specific interface)

User Guidelines

This command effectively enables DiffServ on an interface. No separate interface administrative mode command for DiffServ is available.

Ensure that no attributes within the policy definition exceed the capabilities of the interface. When a policy is attached to an interface successfully, any attempt to change the policy definition, such that it would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Example

The following example shows how to attach a service policy named "DELL" to all interfaces.

```
console(config)#service-policy DELL
```

show class-map

Use the **show class-map** command in Privileged EXEC mode to display all configuration information for the specified class.

Syntax

show class-map [*classname*]

- *classname* — Specifies the valid name of an existing DiffServ class. (Range: 1–31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all the configuration information for the class named "Dell".

```
console#show class-map
```

Class L3			
Class Name	Type	Proto	Reference Class Name
-----	-----	-----	-----
ipv4	All	ipv4	
ipv6	All	ipv6	
stop_http_class	All	ipv6	
match_icmp6	All	ipv6	

```
console#show class-map ipv4
```

```
Class Name..... ipv4
Class Type..... All
Class Layer3 Protocol..... ipv4
```

Match Criteria	Values
-----	-----
Source IP Address	2.2.2.2 (255.255.255.0)

```
console#show class-map stop_http_class
```

```
Class Name..... stop_http_class
Class Type..... All
Class Layer3 Protocol..... ipv6
```

Match Criteria	Values

Source IP Address	2001:DB8::/32
Source Layer 4 Port	80 (http/www)

show classofservice dot1p-mapping

Use the **show classofservice dot1p-mapping** command in Privileged EXEC mode to display the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface.

Syntax

show classofservice dot1p-mapping [*<unit>/<port-type><port>|port-channel port-channel number*]

- *<unit>/<port-type><port>* — Specifies a valid unit/port combination:
 - *<unit>* — Physical switch identifier within the stack. Values are *1-12*.
 - *<port-type>* — Values are *g* for gigabit Ethernet port, or *xg* for 10 gigabit Ethernet port.
 - *<port>* — port number. Values are *1-24* or *1-48* for port_type *g*, and *1-4* for port_type *xg*.

Example: *xg2* is the 10 gigabit Ethernet port 2.

- *port-channel number* — Specifies a valid port-channel number. Range is 1-8.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If the interface is specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Example

The following example displays the dot1p traffic class mapping and user priorities.

```
console#show classofservice dot1p-mapping
```

User	Priority	Traffic Class
-----		-----
0		1
1		1
2		6
3		4
4		3
5		4
6		5
7		6

The following table lists the parameters in the example and gives a description of each.

Parameter	Description
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-dscp-mapping

Use the `show classofservice ip-dscp-mapping` command in Privileged EXEC mode to display the current IP DSCP mapping to internal traffic classes for a specific interface.

Syntax

`show classofservice ip-dscp-mapping`

- Command is supported only globally.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Example

```
console#show classofservice ip-dscp-mapping
```

IP DSCP	Traffic Class
-----	-----
0 (be/cs0)	1
1	1

2	1
3	1
4	1
5	1
6	1
7	1
8 (cs1)	0
9	0
10 (af11)	0
11	0
12 (af12)	0
13	0
14 (af13)	0
15	0
16 (cs2)	0
17	0
18 (af21)	0
19	0
--More-- or (q)uit	
20 (af22)	0
21	0
22 (af23)	0
23	0
24 (cs3)	1
25	1
26 (af31)	1

27	1
28 (af32)	1
29	1
30 (af33)	1
31	1
32 (cs4)	2
33	2
34 (af41)	2
35	2
36 (af42)	2
37	2
38 (af43)	2
39	2
40 (cs5)	2
41	2
42	2
--More-- or (q)uit	
43	2
44	2
45	2
46 (ef)	2
47	2
48 (cs6)	3
49	3
50	3
51	3

52	3
53	3
54	3
55	3
56 (cs7)	3
57	3
58	3
59	3
60	3
61	3
62	3
63	3

console#

show classofservice trust

Use the **show classofservice trust** command in Privileged EXEC mode to display the current trust mode setting for a specific interface.

Syntax

show classofservice trust [*<unit>/<port-type> <port>*] **port-channel** *port-channel number*

- *<unit>/<port-type> <port>* — Specifies a valid unit/port combination:
 - *<unit>* — Physical switch identifier within the stack. Values are *1-12*.
 - *<port-type>* — Values are *g* for gigabit Ethernet port, or *xg* for 10 gigabit Ethernet port.
 - *<port>* — port number. Values are *1-24* or *1-48* for port_type *g*, and *1-4* for port_type *xg*.

Example: *xg2* is the 10 gigabit Ethernet port 2.

- *port-channel number*— Specifies a valid port-channel number. Range is 1-8.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If the interface is specified, the port trust mode of the interface is displayed. If omitted, the port trust mode for global configuration is shown.

Example

The following example displays the current trust mode settings for the specified port.

```
console#show classofservice trust 1/g2
Class of Service Trust Mode: Dot1P
```

show diffserv

Use the **show diffserv** command in Privileged EXEC mode to display the DiffServ general information, which includes the current administrative mode setting as well as the current and maximum number of DiffServ components.

Syntax

show diffserv

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the DiffServ information.

```
console#show diffserv
```

```
DiffServ Admin mode..... Enable
Class Table Size Current/Max..... 5 / 25
Class Rule Table Size Current/Max..... 6 / 150
Policy Table Size Current/Max..... 2 / 64
Policy Instance Table Size Current/Max..... 2 / 640
Policy Attribute Table Size Current/Max.... 2 / 1920
Service Table Size Current/Max..... 26 / 214
```

show diffserv service interface ethernet in

Use the `show diffserv service interface ethernet` command in Privileged EXEC mode to display policy service information for the specified interface.

Syntax

`show diffserv service interface ethernet <unit>/<port-type> <port> in`

- `<unit>/<port-type> <port>` — A valid `<unit>/<port-type> <port>` in the system.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

This command has no user guidelines.

Example

```
console#show diffserv service interface ethernet 1/g1
in
```

```
DiffServ Admin Mode..... Enable
Interface..... 1/g1
Direction..... In
No policy is attached to this interface in this
direction.
```

show diffserv service interface port-channel in

Syntax Description

show diffserv service interface port-channel *channel-group* in

- *channel-group*: A valid port-channel in the system. (Range: 1–18)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

Not applicable

Example

```
console#show diffserv service interface port-channel
1 in
```

```
DiffServ Admin Mode..... Enable
Interface..... ch1
```


Direction..... In
No policy is attached to this interface in this
direction

show diffserv service brief

Use the **show diffserv service brief** command in Privileged EXEC mode to display all interfaces in the system to which a DiffServ policy has been attached.

Syntax

show diffserv service brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display all interfaces in the system to which a DiffServ policy has been attached.

```
console# show diffserv service brief
```

Interface	Direction	OperStatus	Policy Name
-----	-----	-----	-----
1/g1	in	Down	DELL

show interfaces cos-queue

Use the **show interfaces cos-queue** command in Privileged EXEC mode to display the class-of-service queue configuration for the specified interface.

Syntax

show interfaces cos-queue [*<unit>/<port-type> <port>*] **| port-channel**
port-channel number]

- *<unit>/<port-type> <port>* — Specifies a valid unit/port combination:
 - *<unit>* — Physical switch identifier within the stack. Values are *1-12*.
 - *<port-type>* — Values are *g* for gigabit Ethernet port, or *xg* for 10 gigabit Ethernet port.
 - *<port>* — port number. Values are *1-24* or *1-48* for port_type *g*, and *1-4* for port_type *xg*.

Example: *xg2* is the 10 gigabit Ethernet port 2.

- *port-channel number* — Specifies a valid port-channel number. Range is 1-8.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If the interface is specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Examples

The following example displays the COS configuration with no unit/port or port-channel parameter.

```
console#show interfaces cos-queue
```

Global Configuration

Interface Shaping Rate..... 0

Queue Id	Min. Bandwidth	Scheduler Type	Queue Management Type
-----	-----	-----	-----
0	0	Weighted	Tail Drop
1	0	Weighted	Tail Drop
2	0	Weighted	Tail Drop
3	0	Weighted	Tail Drop
4	0	Weighted	Tail Drop
5	0	Weighted	Tail Drop
6	0	Weighted	Tail Drop

This example displays the COS configuration for the specified interface 1/g1.

console#show interfaces cos-queue 1/g1

Interface..... 1/g1

Interface Shaping Rate..... 0

Queue Id	Min. Bandwidth	Scheduler Type	Queue Management Type
-----	-----	-----	-----
0	0	Weighted	Tail Drop
1	0	Weighted	Tail Drop
2	0	Weighted	Tail Drop
3	0	Weighted	Tail Drop
4	0	Weighted	Tail Drop
5	0	Weighted	Tail Drop
6	0	Weighted	Tail Drop

The following table lists the parameters in the examples and gives a description of each.

Parameter	Description
Interface	The port of the interface. If displaying the global configuration, this output line is replaced with a global configuration indication.
Intf Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth values in effect for the interface. This value is a configured value.
Queue Mgmt Type	The queue depth management technique used for all queues on this interface.
Queue	An interface supports n queues numbered 0 to $(n-1)$. The specific n value is platform-dependent. Internal egress queue of the interface; queues 0–6 are available.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This value is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This value is a configured value.

show policy-map

Use the **show policy-map** command in Privileged EXEC mode to display all configuration information for the specified policy.

Syntax

show policy-map [*policyname*]

- *policyname* — Specifies the name of a valid existing DiffServ policy. (Range: 1-31)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the DiffServ information.

```
console#show policy-map
Policy Name    Policy Type    Class Members
-----
POLY1          xxx            DellClass
DELL           xxx            DellClass
```

show policy-map interface

Use the **show policy-map interface** command in Privileged EXEC mode to display policy-oriented statistics information for the specified interface.

Syntax

show policy-map interface *unit/port* **in**

- *unit/port* — Specifies a valid port number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the statistics information for port 1/g1.

```
console#show policy-map interface 1/g1 in
Interface..... 1/g1
Operational Status..... Down
Policy Name..... DELL
Interface Summary:
Class Name..... murali
In Discarded Packets..... 0
Class Name..... test
In Discarded Packets..... 0
Class Name..... DELL1
In Discarded Packets..... 0
Class Name..... DELL
In Discarded Packets..... 0
```

show service-policy

Use the **show service-policy** command in Privileged EXEC mode to display a summary of policy-oriented statistics information for all interfaces.

Syntax

show service-policy in

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary of policy-oriented statistics information.

```
console#show service-policy
```

Intf	Oper Stat	Policy Name

1/g1	Down	DELL
1/g2	Down	DELL
1/g3	Down	DELL
1/g4	Down	DELL
1/g5	Down	DELL
1/g6	Down	DELL
1/g7	Down	DELL
1/g8	Down	DELL
1/g9	Down	DELL
1/g10	Down	DELL

traffic-shape

Use the **traffic-shape** command in Global Configuration mode and Interface Configuration mode to specify the maximum transmission bandwidth limit for the interface as a whole. This process, also known as *rate shaping*, has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. To restore the default interface shaping rate value, use the **no** form of this command.

Syntax

traffic-shape *bw* kbps

no traffic-shape

- *bw* — Maximum transmission bandwidth value expressed in Kbps.
(Range: 64 - 4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the setting of traffic-shape to a maximum bandwidth of 1024 Kbps.

```
console(config-if-1/g1)#traffic-shape 1024 kbps
```


RADIUS Commands

This chapter explains the following commands:

- `aaa accounting network default start-stop group radius`
- `acct-port`
- `auth-port`
- `deadtime`
- `key`
- `msgauth`
- `name`
- `primary`
- `priority`
- `radius-server deadtime`
- `radius-server host`
- `radius-server key`
- `radius-server retransmit`
- `radius-server source-ip`
- `radius-server timeout`
- `retransmit`
- `show radius-servers`
- `show radius-servers statistics`
- `source-ip`
- `timeout`
- `usage`

aaa accounting network default start-stop group radius

Use the `aaa accounting network default start-stop group radius` command to enable RADIUS accounting on the switch. Use the “no” form of this command to disable RADIUS accounting.

Syntax

`aaa accounting network default start-stop group radius`

`no aaa accounting network default start-stop group radius`

Default Configuration

RADIUS accounting is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#aaa accounting network default start-stop group radius
```

acct-port

Use the `acct-port` command to set the port that connects to the RADIUS accounting server. Use the “no” form of this command to reset the port to the default.

Syntax

`acct-port port`

`no acct-port`

- *port* — The layer 4 port number of the accounting server (Range: 1 - 65535).

Default Configuration

The default value of the port number is 1813.

Command Mode

Radius (accounting) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets port number 56 for accounting requests.

```
console(config)#radius-server host acct 3.2.3.2
console(Config-acct-radius)#acct-port 56
```

auth-port

Use the **auth-port** command in Radius mode to set the port number for authentication requests of the designated Radius server.

Syntax

auth-port *auth-port-number*

- *auth-port-number*— Port number for authentication requests. (Range: 1 - 65535)

Default Configuration

The default value of the port number is 1812.

Command Mode

Radius mode

User Guidelines

The host is not used for authentication if set to 0.

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example sets the port number 2412 for authentication requests.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#auth-port 2412
```

deadtime

Use the **deadtime** command in Radius mode to improve Radius response times when a server is unavailable by causing the unavailable server to be skipped.

Syntax

deadtime *deadtime*

- *deadtime* — The amount of time that the unavailable server is skipped over. (Range: 0-2000 minutes)

Default Configuration

The default deadtime interval is 0 minutes.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies a deadtime interval of 60 minutes.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#deadtime 60
```

key

Use the **key** command to specify the encryption key which is shared with the RADIUS server. Use the "no" form of this command to remove the key.

Syntax

key *key-string*

- *key-string* — A string specifying the encryption key (Range: 0 - 128 characters).

Default Configuration

There is no key configured by default.

Command Mode

Radius mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies an authentication and encryption key of “*lion-king*”.

```
console(config)#radius-server host acct 3.2.3.2
console(Config-acct-radius)#key keyacct
```

msgauth

Use the **msgauth** command to enable the message authenticator attribute to be used for the RADIUS Authenticating server being configured. Use the “no” form of this command to disable the message authenticator attribute.

Syntax

msgauth

no msgauth

Default Configuration

The message authenticator attribute is enabled by default.

Command Mode

Radius mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(Config-auth-radius)#msgauth
```

name

Use the **name** command to assign a name to a RADIUS server. Use the "no" form of this command to reset the name to the default.

Syntax

name *servername*

no name

servername — The name for the RADIUS server (Range: 1 - 32 characters).

Default Configuration

The default RADIUS server name is Default-RADIUS-Server.

Command Mode

Radius mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#radius-server host acct 3.2.3.2
console(Config-acct-radius)#name acct777
```

primary

Use the **primary** command to specify that a configured server should be the primary server in the group of authentication servers which have the same server name. Multiple primary servers can be configured for each group of servers which have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of the specified name, it uses the primary server that has the specified server name by default. If it fails to communicate with the primary server for any reason, it uses the backup servers configured with the same server name. These backup servers are identified as the “Secondary” type.

Syntax

primary

Default Configuration

There is no primary authentication server by default.

Command Mode

Radius mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(Config-auth-radius) #primary
```

priority

Use the **priority** command in Radius mode to specify the order in which the servers are to be used, with 0 being the highest priority.

Syntax

priority *priority*

- *priority* — Sets server priority level. (Range 0-65535)

Default Configuration

The default priority is 0.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies a priority of 10 for the designated server.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#priority 10
```

radius-server deadtime

Use the **radius-server deadtime** command in Global Configuration mode to improve Radius response times when servers are unavailable. The command is used to cause the unavailable servers to be skipped. To set the deadtime to 0, use the **no** form of this command.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

- *deadtime* — Length of time in minutes, for which a Radius server is skipped over by transaction requests. (Range: 0–2000 minutes)

Default Configuration

The default dead time is 0 minutes.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the interval for which any unavailable Radius servers are skipped over by transaction requests to 10 minutes.

```
console (config) #radius-server deadtime 10
```

radius-server host

Use the **radius-server host** command in Global Configuration mode to specify a RADIUS server host and enter RADIUS Configuration mode. To delete the specified Radius host, use the **no** form of this command.

Syntax

radius-server host [**acct** | **auth**] {*ipaddress* | *hostname*}

- **acct** | **auth** — The type of server (accounting or authentication).
- *ipaddress* — The RADIUS server host IP address.
- *hostname* — Host name of the Radius server host (Range: 1–255 characters).

Default Configuration

The default server type is authentication. The default server name is “Default RADIUS Server”. The default port number is 1812 for an authentication server and 1813 for an accounting server.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies a Radius server host with the following characteristics:

Server host IP address — 192.168.10.1

```
console(config)#radius-server host 192.168.10.1
```

radius-server key

Use the **radius-server key** command in Global Configuration mode to set the authentication and encryption key for all Radius communications between the switch and the Radius server. To reset to the default, use the **no** form of this command.

Syntax

radius-server key *[key-string]*

no radius-server key

- *key-string*— Specifies the authentication and encryption key for all Radius communications between the switch and the Radius server. This key must match the encryption used on the Radius server. (Range: 1-128 characters)

Default Configuration

The default is an empty string.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the authentication and encryption key for all Radius communications between the device and the Radius server to “dell-server.”

```
console(config)#radius-server key dell-server
```

radius-server retransmit

Use the **radius-server retransmit** command in Global Configuration mode to specify the number of times the Radius client will retransmit requests to the Radius server. To reset the default configuration, use the **no** form of this command.

Syntax

radius-server retransmit *retries*

no radius-server retransmit

- *retries* — Specifies the retransmit value. (Range: 1–10)

Default Configuration

The default is 3 attempts.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the number of times the Radius client attempts to retransmit requests to the Radius server to 5 attempts.

```
console(config)#radius-server retransmit 5
```

radius-server source-ip

Use the **radius-server source-ip** command in Global Configuration mode to specify the source IP address used for communication with Radius servers. To return to the default, use the **no** form of this command. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.

Syntax

radius-server source-ip *source*

no radius-server source-ip

- *source* — Specifies the source IP address.

Default Configuration

The default IP address is the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the source IP address used for communication with Radius servers to 10.1.1.1.

```
console(config)#radius-server source-ip 10.1.1.1
```

radius-server timeout

Use the **radius-server timeout** command in Global Configuration mode to set the interval for which a switch waits for a server host to reply. To restore the default, use the **no** form of this command.

Syntax

radius-server timeout *timeout*

no radius-server timeout

- *timeout* — Specifies the timeout value in seconds. (Range: 1–30)

Default Configuration

The default value is 3 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the interval for which a switch waits for a server host to reply to 5 seconds.

```
console(config)#radius-server timeout 5
```

retransmit

Use the **retransmit** command in Radius mode to specify the number of times the Radius client retransmits requests to the Radius server.

Syntax

retransmit *retries*

- *retries* — Specifies the retransmit value. (Range: 1-10 attempts)

Default Configuration

The default number for attempts is 3.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example of the retransmit command specifies five retries.

```
console(config)#radius-server host 192.143.120.123  
console(config-radius)#retransmit 5
```

show radius-servers

Use the `show radius-servers` command to display the list of configured RADIUS servers and the values configured for the global parameters of the RADIUS client.

Syntax

`show radius-servers [accounting | authentication] [name [servername]]`

accounting — This optional parameter will cause accounting servers to be displayed.

authentication — This optional parameter will cause authentication servers to be displayed.

name — This optional parameter will cause the server names to be displayed instead of the server configuration parameters.

servername — Will cause only the server(s) with *server-name* name to be displayed. There are no global parameters displayed when this parameter is specified.

Default Configuration

Authentication servers are displayed by default.

Command Mode

Privileged EXEC mode

User Guidelines

The following fields are displayed:

Field	Description
Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Named Authentication Server Groups	The number of configured named RADIUS server groups.

Field	Description
Named Accounting Server Groups	The number of configured named RADIUS server groups.
Timeout	The configured timeout value, in seconds, for request retransmissions.
Retransmit	The configured value of the maximum number of times a request packet is retransmitted.
Deadtime	The length of time an unavailable RADIUS server is skipped.
RADIUS Accounting Mode	A Global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A Global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A Global parameter that specifies the IP address to be used in NAS-IP-Address attribute to be used in RADIUS requests.

Example

```
console#show radius-servers

IP address      Type  Port  TimeOut Retran. DeadTime  Source IP
Prio. Usage
-----
--

10.27.5.157    Auth 1812  Global  Global  Global  10.27.65.13  0
all

Global values
Configured Authentication Servers : 1
Configured Accounting Servers : 0
Named Authentication Server Groups : 1
Named Accounting Server Groups : 0
Timeout : 3
```

```
Retransmit : 3
Deadtime : 0
Source IP : 0.0.0.0
RADIUS Attribute 4 Mode : Disable
RADIUS Attribute 4 Value : 0.0.0.0
```

```
console#show radius-servers accounting name
```

Server Name	Host Address	Port	Type
Default-RADIUS-Server	2.2.2.2	1813	Secondary

```
console#show radius-servers name Default-RADIUS-Server
```

```
RADIUS Server Name..... Default-RADIUS-Server
Current Server IP Address..... 1.1.1.1
Retransmits..... 4
Timeout..... 5
Deadtime..... 0
Port..... 1812
Source IP..... 0.0.0.0
Secret Configured..... No
Message Authenticator..... Enable
```


show radius-servers statistics

Use the `show radius-servers statistics` command to show the statistics for an authentication or accounting server.

Syntax

`show radius-servers statistics [accounting | authentication] {ipaddress | hostname | name servername}`

- **accounting | authentication** — The type of server (accounting or authentication).
- *ipaddress* — The RADIUS server host IP address.
- *hostname* — Host name of the Radius server host (Range: 1–158 characters).
- *servername* — The alias used to identify the server.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The following fields are displayed for accounting servers:

Field	Description
RADIUS Accounting Server Name	Name of the accounting server.
Server Host Address	IP address of the host.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting Response and the Accounting Request that matched it from this RADIUS accounting server.

Field	Description
Requests	The number of RADIUS Accounting Request packets sent to this server not including the retransmissions.
Retransmissions	The number of RADIUS Accounting Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts on this server.
Unknown Types	The number of packets unknown type which were received from this server on accounting port.
Packets Dropped	The number of RADIUS packets received from this server on accounting port and dropped for some other reason.

The following fields are displayed for authentication servers:

Field	Description
RADIUS Server Name	Name of the authenticating server.
Server Host Address	IP address of the host.
Access Requests	The number of RADIUS Access Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access Request packets retransmitted to this RADIUS authentication server.

Field	Description
Access Accepts	The number of RADIUS Access Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on authentication port and dropped for some other reason.

Example

```
console#show radius-server statistics accounting
192.168.37.200
```

```
RADIUS Accounting Server Name.....
Default_RADIUS_Server
Host Address.....
192.168.37.200
Round Trip Time..... 0.00
Requests..... 0
```

```
Retransmissions..... 0
Responses..... 0
Malformed Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

```
console#show radius-server statistics name
Default_RADIUS_Server
```

```
RADIUS Server Name..... Default_RADIUS_Server
Server Host Address..... 192.168.37.200
Access Requests..... 0.00
Access Retransmissions..... 0
Access Accepts..... 0
Access Rejects..... 0
Access Challenges..... 0
Malformed Access Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

source-ip

Use the **source-ip** command in Radius mode to specify the source IP address to be used for communication with Radius servers. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.

Syntax

source-ip *source*

- *source* — A valid source IP address.

Default Configuration

The IP address is of the outgoing IP interface.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies 10.240.1.23 as the source IP address.

```
console(config)#radius-server host 192.143.120.123
```

```
console(config-radius)#source-ip 10.240.1.23
```

timeout

Use the **timeout** command in Radius mode to set the timeout value in seconds for the designated Radius server.

Syntax

timeout *timeout*

- *timeout* — Timeout value in seconds for the specified server. (Range: 1-30 seconds.)

Default Configuration

The default value is 3 seconds.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies the timeout setting for the designated Radius Server.

```
console(config)#radius-server host 192.143.120.123
console(config-radius)#timeout 20
```

usage

Use the **usage** command in Radius mode to specify the usage type of the server.

Syntax

usage *type*

- *type* — Variable can be one of the following values: *login*, *802.1x* or *all*.

Default Configuration

The default variable setting is *all*.

Command Mode

Radius mode

User Guidelines

User must enter the mode corresponding to a specific Radius server before executing this command.

Example

The following example specifies usage type *login*.

```
console(config)#radius-server host 192.143.120.123  
console(config-radius)#usage login
```


Spanning Tree Commands

This chapter explains the following commands:

- clear spanning-tree detected-protocols
- exit (mst)
- instance (mst)
- name (mst)
- revision (mst)
- show spanning-tree
- show spanning-tree summary
- spanning-tree
- spanning-tree auto-portfast
- spanning-tree bpdu flooding
- spanning-tree bpdu-protection
- spanning-tree cost
- spanning-tree disable
- spanning-tree forward-time
- spanning-tree guard
- spanning-tree loopguard
- spanning-tree max-age
- spanning-tree max-hops
- spanning-tree mode
- spanning-tree mst 0 external-cost
- spanning-tree mst configuration
- spanning-tree mst cost
- spanning-tree mst port-priority
- spanning-tree mst priority
- spanning-tree portfast

- spanning-tree portfast bpdupfilter default
- spanning-tree portfast default
- spanning-tree port-priority
- spanning-tree priority
- spanning-tree tnguard
- spanning-tree transmit hold-count

clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** command in Privileged EXEC mode to restart the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

Syntax

clear spanning-tree detected-protocols [**ethernet** *interface*] **port-channel** *port-channel-number*]

- *interface* — A valid Ethernet port. The full syntax is: *unit/port*.
- *port-channel-number* — A valid port channel.

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC mode

User Guidelines

This feature is used only when working in RSTP or MSTP mode.

Example

The following example restarts the protocol migration process (forces the renegotiation with neighboring switches) on 1/g1.

```
console#clear spanning-tree detected-protocols  
ethernet 1/g1
```

exit (mst)

Use the **exit** command in MST mode to exit the MST configuration mode and apply all configuration changes.

Syntax

exit

Default Configuration

MST configuration.

Command Mode

MST mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to exit the MST configuration mode and save changes.

```
console(config)#spanning-tree mst configuration
console(config-mst)#exit
```

instance (mst)

Use the **instance** command in MST mode to map VLANs to an MST instance.

Syntax

instance *instance-id* {**add** | **remove**} **vlan** *vlan-range*

- *instance-ID* — ID of the MST instance. (Range: 1-15)
- *vlan-range* — VLANs to be added to the existing MST instance. To specify a range of VLANs, use a hyphen. To specify a series of VLANs, use a comma. (Range: 1-4093)

Default Configuration

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Mode

MST mode

User Guidelines

Before mapping VLANs to an instance use the **spanning-tree mst enable** command to enable the instance.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
console(config)#spanning-tree mst configuration
console(config-mst)#instance 1 add vlan 10-20
```

name (mst)

Use the **name** command in MST mode to define the configuration name. To return to the default setting, use the **no** form of this command.

Syntax

name *string*

- *string* — *Case sensitive* MST configuration name. (Range: 1-32 characters)

Default Configuration

Bridge address.

Command Mode

MST mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the configuration name to “region1”.

```
console(config)#spanning-tree mst configuration
console(config-mst)#name region1
```

revision (mst)

Use the **revision** command in MST mode to identify the configuration revision number. To return to the default setting, use the **no** form of this command.

Syntax

revision *value*

no revision

- *value* — Configuration revision number. (Range: 0-65535)

Default Configuration

Revision number is 0.

Command Mode

MST mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the configuration revision to 1.

```
console(config)#spanning-tree mst configuration
console(config-mst)#revision 1
```

show spanning-tree

Use the **show spanning-tree** command in Privileged EXEC mode to display the spanning-tree configuration.

Syntax

`show spanning-tree [ethernet interface-number | port-channel port-channel-number] [/instance instance-id]`

`show spanning-tree [detail] [active | blockedports] | [instance instance-id]`

`show spanning-tree mst-configuration`

- **detail** — Displays detailed information.
- **active** — Displays active ports only.
- **blockedports** — Displays blocked ports only.
- **mst-configuration** — Displays the MST configuration identifier.
- *interface-number* — A valid Ethernet port number.
- *port-channel-number* — A valid port-channel index.
- *instance -id* — ID of the spanning -tree instance.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display spanning-tree information.

```
console#show spanning-tree
```

```
Spanning tree Disabled BPDU Flooding disabled Portfast  
BPDU filtering Disabled
```

```
mode rstp
```

```
CST Regional Root:          80:00:00:FC:E3:90:00:5D
```

```
Regional Root Path Cost: 0
```

```
ROOT ID
```

Address 80:00:00:FC:E3:90:00:5D

This Switch is the Root.

Hello Time 2 Sec Max Age 20 sec Forward
Delay 15 sec TxHoldCount 6
sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Restricted
1/g1	Enabled	128.1	0	DIS	Disb	No	No
1/g2	Enabled	128.2	0	DIS	Disb	No	No
1/g3	Enabled	128.3	0	DIS	Disb	No	No
1/g4	Enabled	128.4	0	DIS	Disb	No	No

--More-- or (q)uit

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Restricted
1/g5	Enabled	128.5	0	DIS	Disb	No	No
1/g6	Enabled	128.6	0	DIS	Disb	No	No
1/g7	Enabled	128.7	0	DIS	Disb	No	No
1/g8	Enabled	128.8	0	DIS	Disb	No	No
1/g9	Enabled	128.9	0	DIS	Disb	No	No
1/g10	Enabled	128.10	0	DIS	Disb	No	No
1/g11	Enabled	128.11	0	DIS	Disb	No	No
1/g12	Enabled	128.12	0	DIS	Disb	No	No
1/g13	Enabled	128.13	0	DIS	Disb	No	No
1/g14	Enabled	128.14	0	DIS	Disb	No	No
1/g15	Enabled	128.15	0	DIS	Disb	No	No
1/g16	Enabled	128.16	0	DIS	Disb	No	No
1/g17	Enabled	128.17	0	DIS	Disb	No	No
1/g18	Enabled	128.18	0	DIS	Disb	No	No

1/g19	Enabled	128.19	0	DIS	Disb	No	No
1/g20	Enabled	128.20	0	DIS	Disb	No	No

--More-- or (q)uit

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Restricted
-----	-----	-----	-----	----	-----	-----	-----
1/g21	Enabled	128.21		0	DIS	Disb	No
1/g22	Enabled	128.22		0	DIS	Disb	No
1/g23	Enabled	128.23		0	DIS	Disb	No
1/g24	Enabled	128.24		0	DIS	Disb	No
1/xg1	Enabled	128.25		0	DIS	Disb	No
1/xg2	Enabled	128.26		0	DIS	Disb	No
1/xg3	Enabled	128.27		0	DIS	Disb	No
1/xg4	Enabled	128.28		0	DIS	Disb	No
ch1	Enabled	128.626		0	DIS	Disb	No
ch2	Enabled	128.627		0	DIS	Disb	No
ch3	Enabled	128.628		0	DIS	Disb	No
ch4	Enabled	128.629		0	DIS	Disb	No
ch5	Enabled	128.630		0	DIS	Disb	No
ch6	Enabled	128.631		0	DIS	Disb	No
ch7	Enabled	128.632		0	DIS	Disb	No

--More-- or (q)uit

/*****
*****/

```

console(config)#
console#show spanning-tree

Spanning tree Enabled BPDU Flooding disabled Portfast BPDU
filtering Disabled mode rstp

CST Regional Root:          80:00:00:FC:E3:90:00:5D

```

Regional Root Path Cost: 0

ROOT ID

Address 40:00:00:FC:E3:90:06:0F

Path Cost 20000

Root Port 1/g1

Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec

TxHoldCount 6

sec

Bridge ID

Priority 32768

Address 80:00:00:FC:E3:90:00:5D

Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast
Restricted						

--More-- or (q)uit

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast
Restricted						

1/g1	Enabled	128.1	20000	FWD	Root	No	No
1/g2	Enabled	128.2	0	DIS	Disb	No	No
1/g3	Enabled	128.3	200000	DSC	Desg	No	No
1/g4	Enabled	128.4	20000	DSC	Altn	No	No
1/g5	Enabled	128.5	20000	DSC	Altn	No	No
1/g6	Enabled	128.6	0	DIS	Disb	No	No
1/g7	Enabled	128.7	0	DIS	Disb	No	No
1/g8	Enabled	128.8	0	DIS	Disb	No	No
1/g9	Enabled	128.9	0	DIS	Disb	No	No
1/g10	Enabled	128.10	0	DIS	Disb	No	No
1/g11	Enabled	128.11	0	DIS	Disb	No	No

1/g12	Enabled	128.12	0	DIS	Disb	No	No
1/g13	Enabled	128.13	0	DIS	Disb	No	No
1/g14	Enabled	128.14	0	DIS	Disb	No	No
1/g15	Enabled	128.15	0	DIS	Disb	No	No
1/g16	Enabled	128.16	0	DIS	Disb	No	No

--More-- or (q)uit

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	
Restricted							

1/g17	Enabled	128.17	0	DIS	Disb	No	No
1/g18	Enabled	128.18	0	DIS	Disb	No	No
1/g19	Enabled	128.19	0	DIS	Disb	No	No
1/g20	Enabled	128.20	0	DIS	Disb	No	No
1/g21	Enabled	128.21	0	DIS	Disb	No	No
1/g22	Enabled	128.22	0	DIS	Disb	No	No
1/g23	Enabled	128.23	0	DIS	Disb	No	No
1/g24	Enabled	128.24	0	DIS	Disb	No	No
1/xg1	Enabled	128.25	0	DIS	Disb	No	No
1/xg2	Enabled	128.26	0	DIS	Disb	No	No
1/xg3	Enabled	128.27	0	DIS	Disb	No	No
1/xg4	Enabled	128.28	0	DIS	Disb	No	No
ch1	Enabled	128.626	0	DIS	Disb	No	No
ch2	Enabled	128.627	0	DIS	Disb	No	No
ch3	Enabled	128.628	0	DIS	Disb	No	No

--More-- or (q)uit

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	
Restricted							

ch4	Enabled	128.629	0	DIS	Disb	No	No
ch5	Enabled	128.630	0	DIS	Disb	No	No

ch6	Enabled	128.631	0	DIS	Disb	No	No
ch7	Enabled	128.632	0	DIS	Disb	No	No
ch8	Enabled	128.633	0	DIS	Disb	No	No
ch9	Enabled	128.634	0	DIS	Disb	No	No
ch10	Enabled	128.635	0	DIS	Disb	No	No
ch11	Enabled	128.636	0	DIS	Disb	No	No
ch12	Enabled	128.637	0	DIS	Disb	No	No
ch13	Enabled	128.638	0	DIS	Disb	No	No
ch14	Enabled	128.639	0	DIS	Disb	No	No
ch15	Enabled	128.640	0	DIS	Disb	No	No
ch16	Enabled	128.641	0	DIS	Disb	No	No
ch17	Enabled	128.642	0	DIS	Disb	No	No
ch18	Enabled	128.643	0	DIS	Disb	No	No
ch19	Enabled	128.644	0	DIS	Disb	No	No

--More-- or (q)uit

```

/*****
*****/

```

```

console#show spanning-tree active

```

```

Spanning tree Enabled (BPDU flooding : Disabled) Portfast BPDU
filtering Disabl

```

```

ed mode rstp

```

```

CST Regional Root:          80:00:00:FC:E3:90:00:5D

```

```

Regional Root Path Cost:    0

```

```

##### MST 0 Vlan Mapped:    1, 3001

```

```

ROOT ID

```

```

        Address          40:00:00:FC:E3:90:06:0F

```

```

        Path Cost        20000

```

```

        Root Port        1/g1

```

```

        Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec

```

```

Bridge ID

```

```

Priority          32768
Address           80:00:00:FC:E3:90:00:5D
Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec

```

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	RestrictedPort
-----	-----	-----	-----	----	-----	-----	-----

--More-- or (q)uit

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	RestrictedPort
-----	-----	-----	-----	----	-----	-----	-----

1/g1	Enabled	128.1	20000	FWD	Root	No	No
1/g3	Enabled	128.3	200000	FWD	Desg	No	No
1/g4	Enabled	128.4	20000	DSC	Altn	No	No
1/g5	Enabled	128.5	20000	DSC	Altn	No	No

console#

```

/*****
*****/

```

console#show spanning-tree blockedports

Spanning tree Enabled (BPDU flooding : Disabled) mode rstp

CST Regional Root: 80:00:00:FC:E3:90:00:5D

Regional Root Path Cost: 0

MST 0 Vlan Mapped: 1, 3001

ROOT ID

```

Address          40:00:00:FC:E3:90:06:0F
Path Cost        20000
Root Port        1/g1

```

```

Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
Bridge ID
Priority          32768
Address          80:00:00:FC:E3:90:00:5D
Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
Interfaces

  Name      State    Prio.Nbr    Cost        Sts  Role PortFast
RestrictedPort
-----
--More-- or (q)uit

```

```

  Name      State    Prio.Nbr    Cost        Sts  Role PortFast
RestrictedPort
-----
1/g4      Enabled  128.4      20000      DSC  Altn      No      No
1/g5      Enabled  128.5      20000      DSC  Altn      No      No

```

show spanning-tree summary

Use the `show spanning-tree summary` command to display spanning tree settings and parameters for the switch.

Syntax

`show spanning-tree summary`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The following fields are displayed:

Spanning Tree Admin Mode	Enabled or disabled
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the mode parameter.
BPDU Protection Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
BPDU Flooding Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

Example

```
console#show spanning-tree summary
```

```
Spanning Tree Admin Mode..... Disabled
Spanning Tree Version..... IEEE 802.1s
BPDU Protection Mode..... Disabled
BPDU Filter Mode..... Disabled
BPDU Flooding Mode..... Disabled
Configuration Name..... 00-11-88-2B-40-91
```

```
Configuration Revision Level..... 0
Configuration Digest Key.....
0xac36177f50283cd4b83821d8ab26de62
Configuration Format Selector..... 0
No MST instances to display.
```

spanning-tree

Use the **spanning-tree** command in Global Configuration mode to enable spanning-tree functionality. To disable spanning-tree functionality, use the **no** form of this command.

Syntax

```
spanning-tree
no spanning-tree
```

Default Configuration

Spanning-tree is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables spanning-tree functionality.

```
console(config)#spanning-tree
```


spanning-tree auto-portfast

Use the **spanning-tree auto-portfast** command to set the port to auto portfast mode. This enables the port to become a portfast port if it does not see any BPDUs for 3 seconds. Use the “no” form of this command to disable auto portfast mode.

Syntax

spanning-tree auto-portfast

no spanning-tree auto-portfast

Default Configuration

Auto portfast mode is disabled by default.

Command Mode

Interface Configuration (Ethernet, Port Channel) mode

Usage Guidelines

There are no user guidelines for this command.

Example

The following example enables spanning-tree functionality on ethernet interface 4/g1.

```
console#config
```

```
console(config)#interface ethernet 4/g1
```

```
console(config-if-4/g1)#spanning-tree auto-portfast
```

spanning-tree bpdud flooding

The **spanning-tree bpdud flooding** command allows flooding of BPDUs received on non-spanning-tree ports to all other non-spanning-tree ports. Use the “no” form of the command to disable flooding.

Syntax

spanning-tree bpdud flooding

no spanning-tree bpdu flooding

Default Configuration

This feature is disabled by default.

Command Mode

Global Configuration mode

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#spanning-tree bpdu flooding
```

spanning-tree bpdu-protection

Use the **spanning-tree bpdu-protection** command in Global Configuration mode to enable BPDU protection on a switch. Use the **no** form of this command to resume the default status of BPDU protection function.

For an access layer device, the access port is generally connected to the user terminal (such as a desktop computer) or file server directly and configured as an edge port to implement the fast transition. When the port receives a BPDU packet, the system sets it to non-edge port and recalculates the spanning tree, which causes network topology flapping. In normal cases, these ports do not receive any BPDU packets. However, someone may forge BPDU to maliciously attack the switch and cause network flapping.

RSTP provides BPDU protection function against such attack. After BPDU protection function is enabled on a switch, the system disables an edge port that has received BPDU and notifies the network manager about it. The disabled port can only be enabled by the **no** version of the command.

Syntax

spanning-tree bpdu-protection

no spanning-tree bpdu-protection

Default Configuration

BPDU protection is not enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables BPDU protection.

```
console(config)#spanning-tree bpdut-protection
```

spanning-tree cost

Use the **spanning-tree cost** command in Interface Configuration mode to configure the spanning-tree path cost for a port. To return to the default port path cost, use the **no** form of this command.



The command "spanning-tree mst 0 external-cost" on page 553 is used to set path cost for rstp.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

- *cost* — The port path cost. (Range: 0–200,000,000)

Default Configuration

The default cost is 0, which signifies that the cost is automatically calculated based on port speed.

- **10G Port path cost** — 2000
- **Port Channel** — 20,000
- **1000 mbps (giga)** — 20,000
- **100 mbps** — 200,000
- **10 mbps** — 2,000,000

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning-tree cost on 1/g5 to 35000.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)#spanning-tree cost 35000
```

spanning-tree disable

Use the **spanning-tree disable** command in Interface Configuration mode to disable spanning-tree on a specific port. To enable spanning-tree on a port, use the **no** form of this command.

Syntax

```
spanning-tree disable
no spanning-tree disable
```

Default Configuration

By default, all ports are enabled for spanning-tree.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example disables spanning-tree on 1/g5.

```
console(config)#interface ethernet 1/g5
```

```
console(config-if-1/g5)#spanning-tree disable
```

spanning-tree forward-time

Use the **spanning-tree forward-time** command in Global Configuration mode to configure the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state.

To reset the default forward time, use the **no** form of this command.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

- *seconds* — Time in seconds. (Range: 4–30)

Default Configuration

The default forwarding-time for IEEE Spanning-tree Protocol (STP) is 15 seconds.

Command Mode

Global Configuration mode.

User Guidelines

When configuring the Forward-Time the following relationship should be satisfied:

$$2 * (\text{Forward-Time} - 1) \geq \text{Max-Age}.$$

Example

The following example configures spanning-tree bridge forward time to 25 seconds.

```
console(config)#spanning-tree forward-time 25
```

spanning-tree guard

The **spanning-tree guard** command selects whether loop guard or root guard is enabled on an interface. If neither is enabled, the port operates in accordance with the multiple spanning tree protocol. Use the “no” form of this command to disable loop guard or root guard on the interface.

Syntax

spanning-tree guard {root | loop | none}

- **root** — Enables root guard.
- **loop** — Enables loop guard
- **none** — Disables root and loop guard.

Default Configuration

Neither root nor loop guard is enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel) mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example disables spanning-tree guard functionality on ethernet interface 4/g1.

```
console#config
console(config)#interface ethernet 4/g1
console(config-if-4/g1)#spanning-tree guard none
```

spanning-tree loopguard

Use the **spanning-tree loopguard** command to enable loop guard on all ports. Use the “no” form of this command to disable loop guard on all ports.

Syntax

spanning-tree loopguard default
no spanning-tree loopguard default

Default Configuration

Loop guard is disabled by default.

Command Mode

Global Configuration mode

Usage Guidelines

There are no usage guidelines for this command.

Example

The following example enables spanning-tree loopguard functionality on all ports.

```
console(config)#spanning-tree loopguard default
```

spanning-tree max-age

Use the **spanning-tree max-age** command in Global Configuration mode to configure the spanning-tree bridge maximum age. To reset the default maximum age, use the **no** form of this command.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

- *seconds* -Time in seconds. (Range: 6–40)

Default Configuration

The default max-age for IEEE STP is 20 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the Max-Age the following relationships should be satisfied:

$$2 * (\text{Forward-Time} - 1) \geq \text{Max-Age}$$

$$\text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$$

Example

The following example configures the spanning-tree bridge maximum-age to 10 seconds.

```
console(config)#spanning-tree max-age 10
```

spanning-tree max-hops

Use the **spanning-tree max-hops** command to set the MSTP Max Hops parameter to a new value for the common and internal spanning tree. Use the “no” form of this command to reset the Max Hops to the default.

Syntax

```
spanning-tree max-hops hops
```

```
no spanning-tree max-hops
```

- *hops* — The maximum number of hops to use (Range: 1–127).

Default Configuration

The Maximum number of hops is 20 by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#spanning-tree max-hops 32
```


spanning-tree mode

Use the **spanning-tree mode** command in Global Configuration mode to configure the spanning-tree protocol. To return to the default configuration, use the **no** form of this command.

Syntax

spanning-tree mode {stp | rstp | mstp}

no spanning-tree mode

- **stp** — Spanning Tree Protocol (STP) is enabled.
- **rstp** — Rapid Spanning Tree Protocol (RSTP) is enabled.
- **mstp** — Multiple Spanning Tree Protocol (MSTP) is enabled.

Default Configuration

Rapid Spanning Tree Protocol (RSTP) is supported.

Command Mode

Global Configuration mode

User Guidelines

In RSTP mode the switch would use STP when the neighbor switch is using STP. In MSTP mode the switch would use RSTP when the neighbor switch is using RSTP and would use STP when the neighbor switch is using STP.

Example

The following example configures the spanning-tree protocol to MSTP.

```
console(config)#spanning-tree mode mstp
```

spanning-tree mst 0 external-cost

Use the **spanning-tree mst 0 external-cost** command to set the external cost for the common spanning tree. The external cost is used by the switch when negotiating spanning tree topology outside the region.



Since by default each switch is in its own region, the external cost is considered in determining the spanning tree in the network.



This command is used to configure rstp path cost.

Use the “no” form of this command to reset the external cost to the default.

Syntax

spanning-tree mst 0 external-cost *cost*

no spanning-tree mst 0 external-cost

- *cost* — The external cost of the common spanning tree (Range: 0–200000000).

Default Configuration

The default cost is 0, which signifies that the cost is automatically calculated based on port speed.

Port Channel — 20,000

10 Gbps — 2000

1 Gbps — 20,000

100 Mbps — 200,000

10 Mbps — 2,000,000

Command Mode

Interface Configuration (Ethernet, Port Channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning-tree mst 0 external-cost at 20000.

```
console(config-if-4/g1)#spanning-tree mst 0 external-cost 20000
```

spanning-tree mst configuration

Use the **spanning-tree mst configuration** command in Global Configuration mode to enable configuring an MST region by entering the multiple spanning-tree (MST) mode.

Syntax

spanning-tree mst configuration

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number and the same name.

Example

The following example configures an MST region.

```
console (config)#spanning-tree mst configuration
console (config-mst)#instance 1 add vlan 10-20
console (config-mst)#name region1
console (config-mst)#revision 1
```

spanning-tree mst cost

Use the **spanning-tree mst cost** command in Interface Configuration mode to configure the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. To return to the default port path cost, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* cost *cost*

no spanning-tree mst *instance-id* cost

- *instance-ID* — ID of the spanning -tree instance. (Range: 1-15)

- *cost* — The port path cost. (Range: 0–200,000,000)

Default Configuration

The default value is 0, which signifies that the cost will be automatically calculated based on port speed.

The default configuration is:

- Ethernet (10 Mbps) — 2,000,000
- Fast Ethernet (100 Mbps) — 200,000
- Gigabit Ethernet (1000 Mbps) — 20,000
- Port-Channel — 20,000

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the MSTP instance 1 path cost for interface 1/g9 to 4.

```
console(config)#interface ethernet 1/g9
console(config-if-1/g9)#spanning-tree mst 1 cost 4
```

spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** command in Interface Configuration mode to configure port priority. To return to the default port priority, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

- *instance-ID* — ID of the spanning-tree instance. (Range: 1-15)

- *priority* — The port priority. (Range: 0–240 in multiples of 16)

Default Configuration

The default port-priority for IEEE MSTP is 128.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the port priority of port 1/g1 to 144.

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#spanning-tree mst 1 port-
priority 144
```

spanning-tree mst priority

Use the **spanning-tree mst priority** command in Global Configuration mode to set the switch priority for the specified spanning-tree instance. To return to the default setting, use the **no** form of this command.

Syntax

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

- *instance-id* — ID of the spanning-tree instance. (Range: 1-15)
- *priority* — Sets the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0-61440)

Default Configuration

The default bridge priority for IEEE STP is 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The switch with the lowest priority is selected as the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
console(config)#spanning-tree mst 1 priority 4096
```

spanning-tree portfast

Use the **spanning-tree portfast** command in Interface Configuration mode to enable PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire. To disable PortFast mode, use the **no** form of this command.

Syntax

spanning-tree portfast

no spanning-tree portfast

Default Configuration

PortFast mode is disabled.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

This command only applies to all ports. The command is to be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operations.

An interface with PortFast mode enabled is moved directly to the spanning tree forwarding state when linkup occurs without waiting the standard forward-time delay.

Example

The following example enables PortFast on 1/g5.

```
console (config) #interface ethernet 1/g5
console (config-if-1/g5) #spanning-tree portfast
```

spanning-tree portfast bpdudfilter default

The **spanning-tree portfast bpdudfilter default** command discards BPDUs received on spanning-tree ports in portfast mode. Use the “no” form of the command to disable discarding.

Syntax

spanning-tree portfast bpdudfilter default

no spanning-tree portfast bpdudfilter default

Default Configuration

This feature is disabled by default.

Command Mode

Global Configuration mode

Usage Guidelines

There are no usage guidelines for this command.

Example

The following example discards BPDUs received on spanning-tree ports in portfast mode.

```
console#spanning-tree portfast bpdudfilter default
```

spanning-tree portfast default

Use the **spanning-tree portfast default** command to enable Portfast mode only on access ports. Use the “no” form of this command to disable Portfast mode on all ports.

Syntax

spanning-tree portfast default

no spanning-tree portfast default

Default Configuration

Portfast mode is disabled by default.

Command Mode

Global Configuration mode

Usage Guidelines

There are no usage guidelines for this command.

Example

The following example enables Portfast mode on all ports.

```
console(config)#spanning-tree portfast default
```

spanning-tree port-priority

Use the **spanning-tree port-priority** command in Interface Configuration mode to configure port priority. To reset the default port priority, use the **no** form of this command.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

- *priority* — The port priority. (Range: 0–240)

Default Configuration

The default port-priority for IEEE STP is 128.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the spanning priority on 1/g5 to 96.

```
console(config)#interface ethernet 1/g5
console(config-if-1/g5)#spanning-tree port-priority
96
```

spanning-tree priority

Use the **spanning-tree priority** command in Global Configuration mode to configure the spanning-tree priority. The priority value is used to determine which bridge is elected as the root bridge. To reset the default spanning-tree priority use the **no** form of this command.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

- *priority* — Priority of the bridge. (Range: 0–61440)

Default Configuration

The default bridge priority for IEEE STP is 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

Example

The following example configures spanning-tree priority to 12288.

```
console(config)#spanning-tree priority 12288
```

spanning-tree tcnguard

Use the **spanning-tree tcnguard** command to prevent a port from propagating topology change notifications. Use the “no” form of the command to enable TCN propagation.

Syntax

spanning-tree tcnguard

no spanning-tree tcnguard

Default Configuration

TCN propagation is disabled by default.

Command Mode

Interface Configuration (Ethernet, Port Channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures spanning-tree tcnguard on 4/g1.

```
console(config-if-4/g1)#spanning-tree tcnguard
```

spanning-tree transmit hold-count

Use the **spanning-tree transmit hold-count** command to set the maximum number of BPDUs that a bridge is allowed to send within a hello time window (2 seconds). Use the “no” form of this command to reset the hold count to the default value.

Syntax

spanning-tree transmit hold-count [*value*]

no spanning-tree transmit hold-count

- *value* — The maximum number of BPDUs to send (Range: 1–10).

Default Configuration

The default hold count is 6 BPDUs.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the maximum number of BPDUs sent to 6.

```
console(config)#spanning-tree transmit hold-count 6
```


Switchport Voice Commands

This chapter explains the following commands:

- `show switchport voice`
- `switchport voice detect auto`

show switchport voice

Use the `show switchport voice` command to show the status of auto-voip on an interface or all interfaces.

Syntax

`show switchport voice [interface {ethernet interface | port-channel index}]`

- `ethernet interface`—Specifies a valid interface. The full syntax is unit/port.
- `port-channel index`—Specifies the port-channel number.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show switchport voice
```

Interface	Auto VoIP Mode	Traffic Class
-----	-----	-----
1/g1	Enabled	6
1/g2	Enabled	6
1/g3	Enabled	6
1/g4	Enabled	6
1/g5	Enabled	6
1/g6	Enabled	6
1/g7	Enabled	6

1/g8	Enabled	6
1/g9	Enabled	6
1/g10	Enabled	6
1/g11	Enabled	6
1/g12	Enabled	6
1/g13	Enabled	6
1/g14	Enabled	6
1/g15	Enabled	6
1/g16	Enabled	6
1/g17	Enabled	6
1/g18	Enabled	6
1/g19	Enabled	6
1/g20	Enabled	6

--More-- or (q)uit

```
console#show switchport voice ethernet 1/g1
```

Interface	Auto	VoIP	Mode	Traffic	Class

1/g1		Disabled		6	

```
console#show switchport voice port-channel 1
```

Interface	Auto	VoIP	Mode	Traffic	Class

ch1		Disabled		6	

The command output provides the following information:

- **AutoVoIP Mode**—The Auto VoIP mode on the interface.
- **Traffic Class**—The Cos Queue or Traffic Class to which all VoIP traffic is mapped. This is not configurable and defaults to the highest COS queue available in the system for data traffic.

switchport voice detect auto

The **switchport voice detect auto** command is used to enable the VoIP Profile on all the interfaces of the switch (global configuration mode) or for a specific interface (interface configuration mode). Use the “no” form of the command to disable the VoIP Profile.

Syntax

switchport voice detect auto

no switchport voice detect auto

Default Configuration

This feature is disabled by default.

Command Mode

Global Configuration.

Interface (Ethernet, Port-channel) Configuration.

User Guidelines

This command has no user guidelines

Example

```
console(config)#switchport voice detect auto
```

```
console(config-if-1/g1)#switchport voice detect auto
```


TACACS+ Commands

This chapter explains the following commands:

- key
- port
- priority
- show tacacs
- tacacs-server host
- tacacs-server key
- tacacs-server timeout
- timeout

key

Use the **key** command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon.

Syntax

key [key-string]

- key-string — *To specify the key name. (Range: 1–128 characters)*

Default Configuration

If left unspecified, the key-string parameter defaults to the global value.

Command Mode

TACACS Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies an encryption and authentication key of 12.

```
console(config-tacacs)#key 12
```

port

Use the **port** command in TACACS Configuration mode to specify a server port number.

Syntax

port [port-number]

- port-number — *The server port number. If left unspecified, the default port number is 49. (Range: 0–65535)*

Default Configuration

The default port number is 49.

Command Mode

TACACS Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to specify server port number 1200.

```
console(tacacs)#port 1200
```

priority

Use the **priority** command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority.

Syntax

priority [priority]

- *priority* — Specifies the priority for servers. 0 (zero) is the highest priority. (Range: 0–65535)

Default Configuration

If left unspecified, this parameter defaults to 0 (zero).

Command Mode

TACACS Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to specify a server priority of 10000.

```
console(config-tacacs)#priority 10000
```

show tacacs

Use the **show tacacs** command in Privileged EXEC mode to display the configuration and statistics of a TACACS+ server.

Syntax

```
show tacacs [ip-address]
```

- *ip-address* — The name or IP address of the host.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays TACACS+ server settings.

```
console#show tacacs
```

```
Global Timeout: 5
```

IP address	Port	Timeout	Priority
-----	-----	-----	-----
10.254.24.162	49	Global	0

tacacs-server host

Use the **tacacs-server host** command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. To delete the specified hostname or IP address, use the **no** form of this command.

Syntax

tacacs-server host {*ip-address* | *hostname*}

no tacacs-server host {*ip-address* | *hostname*}

- *ip-address* — The IP address of the TACACS+ server.
- *hostname* — The hostname of the TACACS+ server. (Range: 1-255 characters).

Default Configuration

No TACACS+ host is specified.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, multiple **tacacs-server host** commands can be used.

Example

The following example specifies a TACACS+ host.

```
console(config)#tacacs-server host 172.16.1.1
console(tacacs)#
```

tacacs-server key

Use the **tacacs-server key** command in Global Configuration mode to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. To disable the key, use the **no** form of this command.

Syntax

tacacs-server key [*key-string*]

no tacacs-server key

- *key-string* — Specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon. (Range: 0–128 characters)

Default Configuration

The default is an empty string.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the authentication encryption key.

```
console(config)#tacacs-server key dell-s
```

tacacs-server timeout

Use the **tacacs-server timeout** command in Global Configuration mode to set the interval during which a switch waits for a server host to reply. To restore the default, use the **no** form of this command.

Syntax

tacacs-server timeout [*timeout*]

no tacacs-server timeout

- *timeout* — The timeout value in seconds. (Range: 1–30)

Default Configuration

The default value is 5 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the timeout value as 30.

```
console(config)#tacacs-server timeout 30
```

timeout

Use the **timeout** command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used.

Syntax

timeout [timeout]

- *timeout* — The timeout value in seconds. (Range: 1–30)

Default Configuration

If left unspecified, the timeout defaults to the global value.

Command Mode

TACACS Configuration mode

User Guidelines

This command has no user guidelines.

Example

This example shows how to specify the timeout value.

```
console(config-tacacs)#timeout 23
```


VLAN Commands

This chapter explains the following commands:

- `dvlan-tunnel ethertype`
- `interface vlan`
- `interface range vlan`
- `mode dvlan-tunnel`
- `name`
- `protocol group`
- `protocol vlan group`
- `protocol vlan group all`
- `show dvlan-tunnel`
- `show dvlan-tunnel interface`
- `show interfaces switchport`
- `show port protocol`
- `show port protocol`
- `show vlan`
- `show vlan association mac`
- `show vlan association subnet`
- `switchport access vlan`
- `switchport forbidden vlan`
- `switchport general acceptable-frame-type tagged-only`
- `switchport general allowed vlan`
- `switchport general ingress-filtering disable`
- `switchport general pvid`
- `switchport mode`
- `switchport protected`
- `switchport protected name`

- switchport trunk allowed vlan
- vlan
- vlan association mac
- vlan association subnet
- vlan database
- vlan makestatic
- vlan protocol group
- vlan protocol group add protocol
- vlan protocol group name
- vlan protocol group remove
- groupid — The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the vlan protocol group command. To see the group ID associated with the name of a protocol group, use the show port protocol all command.

dvlan-tunnel ethertype

Use the **dvlan-tunnel ethertype** command in Global Configuration mode to configure the ethertype for the specified interface.

To configure the EtherType on the specified interface to its default value, use the **no** form of this command.

Syntax

dvlan-tunnel ethertype {802.1Q | vman | custom <0-65535>}

no dvlan-tunnel ethertype

- 802.1Q — Configures the EtherType as 0x8100.
- vman — Configures the EtherType as 0x88A8.
- custom — Custom configures the EtherType for the DVLAN tunnel. The value must be 0-65535.

Default Configuration

The default for this command is 802.1Q.

Command Mode

Global Configuration

User Guidelines

This command has no user guidelines.

Example

The following example displays configuring Double VLAN tunnel for vman EtherType.

```
console(config)#dvlan-tunnel ethertype vman
```

interface vlan

Use the **interface vlan** command in Global Configuration mode to configure a VLAN type and to enter Interface Configuration mode.

Syntax

interface vlan *vlan-id*

- *vlan-id*— The ID of a valid VLAN (Range: 1–4093).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the VLAN 1 IP address of 131.108.1.27 and subnet mask 255.255.255.0.

```
console(config)#interface vlan 1  
  
console(config-vlan)#ip address 131.108.1.27  
255.255.255.0
```

interface range vlan

Use the **interface range vlan** command in Global Configuration mode to execute a command on multiple VLANs at the same time.

Syntax

interface range vlan { *vlan-range* | **all** }

- *vlan-range* — A list of valid VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 2–4093)
- **all** — All existing static VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands used in the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution continues on other interfaces.

Example

The following example groups VLAN 221 till 228 and VLAN 889 to receive the same command.

```
console(config)#interface range vlan 221-228,889
console(config-if)#
```

mode dvlan-tunnel

Use the **mode dvlan-tunnel** command in Interface Configuration mode to enable Double VLAN Tunneling on the specified interface. To disable Double VLAN Tunneling on the specified interface, use the **no** form of this command.

Syntax

mode dvlan-tunnel

no mode dvlan-tunnel

Default Configuration

By default, Double VLAN Tunneling is *disabled*.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to enable Double VLAN Tunneling at ethernet port 1/g1.

```
console(config-if-1/g1)#mode dvlan-tunnel
```

name

Use the **name** command in Interface Configuration mode to add a name to a VLAN. To remove the VLAN name, use the **no** form of this command.



NOTE: This command cannot be configured for a range of interfaces (range context).

Syntax

name *string*

no name

- *string* — Comment or description to help identify a specific VLAN (Range: 1–32 characters).

Default Configuration

No name is defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The VLAN name must be unique.

Example

The following example names VLAN number 19 with the name "Marketing."

```
console(config)#interface vlan 19
console(config-if-vlan19)#name Marketing
```

protocol group

Use the **protocol group** command in VLAN Database mode to attach a VLAN ID to the protocol-based group identified by *groupid*. A group may only be associated with one VLAN at a time. However, the VLAN association can be changed. The referenced VLAN should be created prior to the creation of the protocol-based group except when GVRP is expected to create the VLAN.

To detach the VLAN from this protocol-based group identified by this *groupid*, use the **no** form of this command.

Syntax

protocol group *groupid* *vlanid*

no protocol group *groupid* *vlanid*

- *groupid*— The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.
- *vlanid*— A valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to attach the VLAN ID "100" to the protocol-based VLAN group "3."

```
console#vlan database
console(config-vlan)#protocol group 3 100
```

protocol vlan group

Use the **protocol vlan group** command in Interface Configuration mode to add the physical unit/port interface to the protocol-based group identified by *groupid*. A group may have more than one interface associated with it. Each interface and protocol combination can be associated with one group only. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group. Ensure that the referenced VLAN is created prior to the creation of the protocol-based group except when GVRP is expected to create the VLAN.

To remove the interface from this protocol-based VLAN group that is identified by this *groupid*, use the **no** form of this command.

If you select **all**, all ports are removed from this protocol group.

Syntax

protocol vlan group *groupid*

no protocol vlan group *groupid*

- *groupid*— The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add a physical port interface to the group ID of "2."


```
console(config-if-1/g1)#protocol vlan group 2
```

protocol vlan group all

Use the **protocol vlan group all** command in Global Configuration mode to add all physical interfaces to the protocol-based group identified by *groupid*. A group may have more than one interface associated with it. Each interface and protocol combination can be associated with one group only. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group. Ensure that the referenced VLAN is created prior to the creation of the protocol-based group except when GVRP is expected to create the VLAN.

To remove all interfaces from this protocol-based group that is identified by this *groupid*, use the **no** form of the command

Syntax

protocol vlan group all *groupid*

no protocol vlan group all *groupid*

- *groupid*— The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add all physical interfaces to the protocol-based group identified by group ID "2."

```
console(config)#protocol vlan group all 2
```

show dvlan-tunnel

Use the **show dvlan-tunnel** command in Privileged EXEC mode to display all interfaces enabled for Double VLAN Tunneling.

Syntax

```
show dvlan-tunnel
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to display all interfaces for Double VLAN Tunneling.

```
console#show dvlan-tunnel
```

```
Interfaces Enabled for DVLAN Tunneling..... 1/g1
```

show dvlan-tunnel interface

Use the **show dvlan-tunnel interface** command in Privileged EXEC mode to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Syntax

```
show dvlan-tunnel interface {unit/port | all}
```

- *unit/port* — A valid unit and port number separated by forward slashes (/).
- **all** — Displays information for all interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays detailed information for unit/port "1/g1."

```
console#show dvlan-tunnel interface 1/g1

Interface   Mode      EtherType
-----
1/g1        Enable    vMAN
```

The following table describes the significant fields shown in the example.

Field	Description
Mode	This field specifies the administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is <i>disabled</i> .
Interface	Interface Number.
EtherType	This field represents a 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. The three different EtherType tags are: (1) 802.1Q, which represents the commonly used value of 0x8100. (2) vMAN, which represents the commonly used value of 0x88A8. (3) If EtherType is not one of these two values, it is a custom tunnel value, representing any value in the range of 0 to 65535.

show interfaces switchport

Use the **show interfaces switchport** command in Privileged EXEC mode to display switchport configuration.

Syntax

show interfaces switchport {ethernet *interface*|port-channel *port-channel-number*}

- *Interface* — Specific interface, such as ethernet 1/g8.
- *port-channel-number* — Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays switchport configuration individually for g1.

```
console#show interface switchport ethernet 1/g1
```

```
Port 1/g1:
```

```
VLAN Membership mode: General
```

```
Operating parameters:
```

```
PVID: 1 (default)
```

```
Ingress Filtering: Enabled
```

```
Acceptable Frame Type: All
```

```
GVRP status: Enabled
```

```
Protected: Enabled
```

```
Port 1/g1 is member in:
```

VLAN	Name	Egress rule	Type
----	-----	-----	-----
1	default	untagged	Default

8	VLAN008	tagged	Dynamic
11	VLAN0011	tagged	Static
19	IPv6 VLAN	untagged	Static
72	VLAN0072	untagged	Static

Static configuration:

PVID: 1 (default)

Ingress Filtering: Enabled

Acceptable Frame Type: All

Port 1/g1 is statically configured to:

VLAN	Name	Egress rule
----	-----	-----
11	VLAN0011	tagged
19	IPv6 VLAN	untagged
72	VLAN0072	untagged

Forbidden VLANs:

VLAN	Name
----	-----
73	Out

The following example displays switchport configuration individually for 1/g2.

```
console#show interface switchport ethernet 1/g2
```

Port 1/g2:

VLAN Membership mode: General

Operating parameters:

PVID: 4095 (discard vlan)

Ingress Filtering: Enabled

Acceptable Frame Type: All

Port 1/g1 is member in:

VLAN	Name	Egress rule	Type
----	-----	-----	-----
91	IP Telephony	tagged	Static

Static configuration:

PVID: 8

Ingress Filtering: Disabled

Acceptable Frame Type: All

Port 1/g2 is statically configured to:

VLAN	Name	Egress rule
----	-----	-----
8	VLAN0072	untagged
91	IP Telephony	tagged

Forbidden VLANs:

VLAN	Name
----	-----
73	Out

The following example displays switchport configuration individually for 2/g19.

console#show interfaces switchport ethernet 2/g19

Port 2/g19:

Operating parameters:

PVID: 2922

Ingress Filtering: Enabled

Acceptable Frame Type: Untagged

GVRP status: Disabled

Port 2/g19 is member in:

VLAN	Name	Egress rule	Type
----	-----	-----	----
2921	Primary A	untagged	Static
2922	Community A1	untagged	Static

Static configuration:

PVID: 2922

Ingress Filtering: Enabled

Acceptable Frame Type: Untagged

GVRP status: Disabled

Port 2/g19 is member in:

VLAN	Name	Egress rule	Type
----	-----	-----	----
2921	Primary A	untagged	Static
2922	Community A1	untagged	Static

show port protocol

Use the **show port protocol** command in Privileged EXEC mode to display the Protocol-Based VLAN information for either the entire system or for the indicated group.

Syntax

show port protocol {*groupid* | **all**}

- *groupid*— The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command.
- **all** — Enter **all** to show all interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the Protocol-Based VLAN information for either the entire system.

```
console#show port protocol all
```

Group				
Name	ID	Protocol(s)	VLAN	Interface(s)

test	1	IP	1	1/g1

show switchport protected

Use the **show switchport protected** command in Privileged EXEC mode to display the status of all the interfaces, including protected and unprotected interfaces.

Syntax

```
show switchport protected groupid
```

- *groupid*— Identifies which group the port is to be protected in. (Range: 0-2)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example identifies test as the protected group.

```
console#show switchport protected 0
Name..... test
```

show vlan

Use the `show vlan` command in Privileged EXEC mode to display VLAN information.

Syntax

```
show vlan [id vlan-id | name vlan-name]
```

- *vlan-id* — A valid VLAN ID.
- *vlan-name* — A valid VLAN name string. (Range: 1–32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all VLAN information.

```
console#show vlan
VLAN      Name                Ports              Type              Authorization
-----
1         default            1/g1-1/g2         Other             Required
```

		2/g1-1/g4		
10	VLAN0010	1/g3-1/g4	dynamic	Required
11	VLAN0011	1/g1-1/g2	static	Required
20	VLAN0020	1/g3-1/g4	static	Required
21	VLAN0021		static	Required
30	VLAN0030		static	Required
31	VLAN0031		static	Required
91	VLAN0011	1/g1-1/g2	static	Not Required
3964	Guest VLAN	1/g17	Guest	-

show vlan association mac

Use the **show vlan association mac** command in Privileged EXEC mode to display the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Syntax

show vlan association mac [*mac-address*]

- *mac-address* — Specifies the MAC address to be entered in the list.
(Range: Any valid MAC address)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows no entry in MAC address to VLAN cross-reference.

```
console#show vlan association mac
```

MAC Address	VLAN ID
-----	-----
0001.0001.0001.0001	1

show vlan association subnet

Use the **show vlan association subnet** command in Privileged EXEC mode to display the VLAN associated with a specific configured IP-Address and netmask. If no IP Address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Syntax

show vlan association subnet [*ip-address ip-mask*]

- *ip-address* — Specifies IP address to be shown
- *ip-mask* — Specifies IP mask to be shown

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The command has no user guidelines.

Example

The following example shows the case if no IP Subnet to VLAN association exists.

```
console#show vlan association subnet
```

IP Address	IP Mask	VLAN ID
-----	-----	-----

The IP Subnet to VLAN association does not exist.

switchport access vlan

Use the **switchport access vlan** command in Interface Configuration mode to configure the VLAN ID when the interface is in access mode. To reconfigure the default, use the **no** form of this command.

Syntax

switchport access vlan *vlan-id*

no switchport access vlan

- *vlan-id*— A valid VLAN ID of the VLAN to which the port is configured.

Default Configuration

The default value for the *vlan-id* parameter is 1.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command automatically removes the port from the previous VLAN and adds it to the new VLAN.

Example

The following example configures a VLAN ID of interface 1/g8 to become an access member of VLAN ID 23.

```
console(config)#interface ethernet 1/g8
```

```
console(config-if-1/g8)#switchport access vlan 23
```

switchport forbidden vlan

Use the **switchport forbidden vlan** command in Interface Configuration mode to forbid adding specific VLANs to a port. To revert to allowing the addition of specific VLANs to the port, use the **remove** parameter of this command.

Syntax

`switchport forbidden vlan {add vlan-list | remove vlan-list}`

- **add *vlan-list*** — List of valid VLAN IDs to add to the forbidden list. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **remove *vlan-list*** — List of valid VLAN IDs to remove from the forbidden list. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Default Configuration

All VLANs allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example forbids adding VLAN numbers 234 through 256 to port 1/g8.

```
console(config)#interface ethernet 1/g8
```

```
console(config-if-1/g8)#switchport forbidden vlan add  
234-256
```

switchport general acceptable-frame-type tagged-only

Use the `switchport general acceptable-frame-type tagged-only` command in Interface Configuration mode to discard untagged frames at ingress. To enable untagged frames at ingress, use the **no** form of this command.

Syntax

`switchport general acceptable-frame-type tagged-only`

no switchport general acceptable-frame-type tagged-only

Default Configuration

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures 1/g8 to discard untagged frames at ingress.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#switchport general
acceptable-frame-type tagged-only
```

switchport general allowed vlan

Use the **switchport general allowed vlan** command in Interface Configuration mode to add VLANs to or remove VLANs from a general port.

Syntax

switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]

switchport general allowed vlan remove *vlan-list*

- **add** *vlan-list* — List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **remove** *vlan-list* — List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **tagged** — Sets the port to transmit tagged packets for the VLANs. If the port is added to a VLAN without specifying tagged or untagged, the default is untagged.

- **untagged** — Sets the port to transmit untagged packets for the VLANs.

Default Configuration

Untagged.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

You can use this command to change the egress rule (for example, from tagged to untagged) without first removing the VLAN from the list.

Example

The following example shows how to add VLANs 1, 2, 5, and 8 to the allowed list.

```
console(config-if-1/g8)#switchport general allowed  
vlan add 1,2,5,8 tagged
```

switchport general ingress-filtering disable

Use the **switchport general ingress-filtering disable** command in Interface Configuration mode to disable port ingress filtering. To enable ingress filtering on a port, use the **no** form of this command.

Syntax

```
switchport general ingress-filtering disable  
no switchport general ingress-filtering disable
```

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to enable port ingress filtering on 1/g8.

```
console(config)#interface ethernet 1/g8
```

```
console(config-if-1/g8)#switchport general ingress-  
filtering disable
```

switchport general pvid

Use the **switchport general pvid** command in Interface Configuration mode to configure the Port VLAN ID (PVID) when the interface is in general mode. Use the **switchport mode general** command to set the VLAN membership mode of a port to "general." To configure the default value, use the **no** form of this command.

Syntax

```
switchport general pvid vlan-id
```

```
no switchport general pvid
```

- *vlan-id*— PVID. The VLAN ID may belong to a non-existent VLAN.

Default Configuration

The default value for the *vlan-id* parameter is 1 when the VLAN is enabled. Otherwise, the value is 4093.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to configure the PVID for 1/g8, when the interface is in general mode.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#switchport general pvid 234
```

switchport mode

Use the **switchport mode** command in Interface Configuration mode to configure the VLAN membership mode of a port. To reset the mode to the appropriate default for the switch, use the **no** form of this command.

Syntax

switchport mode {access | trunk | general}

no switchport mode

- **access** — An access port connects to a single end station belonging to a single VLAN. An access port is configured with ingress filtering enabled and will accept either an untagged frame or a packet tagged with the access port VLAN. An access port only egresses untagged packets.
- **trunk** — Trunk port connects two switches. A trunk port may belong to multiple VLANs. A trunk port accepts only packets tagged with the VLAN IDs of the VLANs to which the trunk is a member. A trunk only egresses tagged packets.
- **general** — Full 802.1q support VLAN interface. A general mode port may be a combination of both trunk and access ports. It is possible to fully configure all VLAN features on a general mode port.

Default Configuration

The default for this command is **access**.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures 1/g8 to access mode.

```
console(config)#interface ethernet 1/g8
console(config-if-1/g8)#switchport mode access
```

switchport protected

Use the **switchport protected** command in Interface Configuration mode to configure a protected port. The *groupid* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group. You are required to remove an interface from one group before adding it to another group.

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Syntax

switchport protected *groupid*

no switchport protected

- *groupid*—Identifies which group this port will be protected in. (Range: 0-2)

Default Configuration

No protected switchports are defined.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures Ethernet port 1/g1 as a member of protected group 1.

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#switchport protected 1
```

switchport protected name

Use the **switchport protected name** command in Global Configuration mode to add the port to the protected group 1 and also sets the group name to "protected".

Syntax

switchport protected *groupid* **name** *name*

no switchport protected *groupid* **name**

- *groupid*— Identifies which group the port is to be protected in. (Range: 0-2)
- *name* — Name of the group. (Range: 0-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example assigns the name "protected" to group 1.

```
console(config-if-1/g1)#switchport protected 1 name
protected
```

switchport trunk allowed vlan

Use the **switchport trunk allowed vlan** command in Interface Configuration mode to add VLANs to or remove VLANs from a trunk port.

Syntax

switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}

- **add** *vlan-list* — List of VLAN IDs to add. Separate non-consecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **remove** *vlan-list* — List of VLAN IDs to remove. Separate non-consecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command has no user guidelines.

Example

The following example shows how to add VLANs 1, 2, and 5 to 8 to the allowed list.

```
console(config-if-1/g8)#switchport trunk allowed vlan  
add 1,2,5-8
```

vlan

Use the **vlan** command in VLAN Database mode to configure a VLAN. To delete a VLAN, use the **no** form of this command.

Syntax

vlan *vlan-range*

no vlan *vlan-range*

- *vlan-range* — A list of valid VLAN IDs to be added. List separate, non-consecutive VLAN IDs separated by commas (without spaces); use a hyphen to designate a range of IDs. (Range: 2–4093)

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database mode

User Guidelines

Deleting the VLAN for an access port will cause that port to become unusable until it is assigned a VLAN that exists.

Example

The following example shows how to create (add) VLAN of IDs 22, 23, and 56.

```
console(config-vlan)#vlan 22,23,56
```

```
console(config-vlan)#
```

vlan association mac

Use the **vlan association mac** command in VLAN Database mode to associate a MAC address to a VLAN. The maximum number of MAC-based VLANs is 256.

Syntax

vlan association mac *mac-address vlanid*

no vlan association mac *mac-address*

mac-address — MAC address to associate. (Range: Any MAC address in the format xxxx.xxxx.xxxx)

vlanid— VLAN to associate with subnet. (Range: 1-4093)

Default Configuration

No assigned MAC address.

Command Mode

VLAN Database mode

User Guidelines

This command has no user guidelines.

Example

The following example associates MAC address with VLAN ID 1.

```
console(config-vlan)#vlan association mac  
0001.0001.0001 1
```

vlan association subnet

Use the **vlan association subnet** command in VLAN Database mode to associate a VLAN to a specific IP-subnet.

Syntax

vlan association subnet *ip-address subnet-mask vlanid*

no vlan association subnet *ip-address subnet-mask*

- *ip-address* — Source IP address. (Range: Any valid IP address)
- *subnet-mask* — Subnet mask. (Range: Any valid subnet mask)
- *vlanid* — VLAN to associated with subnet. (Range: 1-4093)

Default Configuration

No assigned ip-subnet.

Command Mode

VLAN Database mode

User Guidelines

This command has no user guidelines.

Example

The following example associates IP address with VLAN ID 100.

```
console(config-vlan)#vlan association subnet  
192.245.23.45 255.255.255.0 100
```

vlan database

Use the **vlan database** command in Global Configuration mode to enter the VLAN database configuration mode.

Syntax

vlan database

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters the VLAN database mode.

```
console(config)#vlan database  
console(config-vlan)#
```

vlan makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

Syntax

vlan makestatic *vlan-id*

- *vlan-id*— Valid vlan ID. Range is 2–4093.

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database Mode

User Guidelines

The dynamic VLAN (created via GRVP) should exist prior to executing this command. See the Type column in output from the **show vlan** command to determine that the VLAN is dynamic.

Example

The following changes vlan 3 to a static VLAN.

```
console(config-vlan)#vlan makestatic 3
```

vlan protocol group

Use the **vlan protocol group** command in Global Configuration mode to add protocol-based groups to the system. When a protocol group is created, it is assigned a unique group ID number. The group ID is used to identify the group in subsequent commands. Use the **no** form of the command to remove the specified VLAN protocol group name from the system.

If multiple vlan protocol groups are created, this command deletes one of the groups, and then saves the configuration. The older implementation of this command resulted in incorrectly applying the group IDs on reload. So, the

existing command **vlan protocol group** <groupname> is updated to **vlan protocol group** <groupid> so that **groupid** is used for both configuration and script generation.



NOTE: If an attempt is made to migrate to the latest implementation with any of the groupnames deleted prior to saving configuration on the pre 3.0.0.x code (applicable only for platforms PC62xx, PCM622x, PCM8024), the problem on the latest code will remain.

Syntax

vlan protocol group <groupid>

no vlan protocol group <groupid>

- *groupid*— The protocol-based VLAN group ID, to create a protocol-based VLAN group. To see the created protocol groups, use the show port protocol all command.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console(config)# vlan protocol group 1
```

vlan protocol group add protocol

Use the **vlan protocol group add protocol** command in Global Configuration mode to add a protocol to the protocol-based VLAN groups identified by *groupid*. A group may have more than one protocol associated with it. Each interface and protocol combination can be associated with one group only. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group.

To remove the protocol from the protocol-based VLAN group identified by *groupid*, use the **no** form of this command.

Syntax

vlan protocol group add protocol *<groupid>* *ethertype* *<value>*

no vlan protocol group add protocol *<groupid>* *ethertype* *<value>*

- *groupid*— The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.
- *ethertype*— The protocol you want to add. The ethertype can be any valid hexadecimal number in the range 1536 to 65535.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays how to add the "ip" protocol to the protocol based VLAN group identified as "2."

```
console(config)#vlan protocol group add protocol 2  
ethertype 0xFFFF
```

vlan protocol group name

This is a new command for assigning a group name to **vlan protocol group id**.

Syntax

vlan protocol group name <groupid> <groupName>

no vlan protocol group name <groupid>

- *groupid*—The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command
- *groupName*—The group name you want to add. The group name can be up to 16 characters length. It can be any valid alpha numeric characters.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console(config)# vlan protocol group name 1 usergroup
```

vlan protocol group remove

Use the **vlan protocol group remove** command in Global Configuration mode to remove the protocol-based VLAN group identified by *groupid*.

Syntax

vlan protocol group remove *groupid*

- *groupid* — The protocol-based VLAN group ID, which is automatically generated when you create a protocol-based VLAN group with the **vlan protocol group** command. To see the group ID associated with the name of a protocol group, use the **show port protocol all** command.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the removal of the protocol-based VLAN group identified as "2."

```
console(config)#vlan protocol group remove 2
```

vlan routing

Use the **vlan routing** command to enable routing on a VLAN. Use the “no” form of this command to disable routing on a VLAN.

Syntax

vlan routing *vlanid* [*index*]

- *vlanid*— Valid VLAN ID (Range 1–4093).
- *index* — Internal interface ID. This optional parameter is listed in the configuration file for all VLAN routing interfaces. When a nonstop forwarding failover occurs, this information enables the system to correlate checkpointed state information with the proper interfaces and their configuration.

Default Configuration

Routing is not enabled on any VLANs by default.

Command Mode

VLAN Database mode

User Guidelines

The user is not required to use this command. Routing can still be enabled using the **routing** command in VLAN Interface Configuration mode.

Examples

```
console(config-vlan)# vlan routing 10 1
```


Voice VLAN Commands

This chapter explains the following commands:

- voice vlan
- voice vlan (Interface)
- voice vlan data priority
- show voice vlan

voice vlan

This command is used to enable the voice vlan capability on the switch.

Syntax

voice vlan

no voice vlan

Parameter Ranges

Not applicable

Command Mode

Global Configuration

Usage Guidelines

Not applicable

Default Value

This feature is disabled by default.

Example

```
console(config)#voice vlan
```

```
console(config)#no voice vlan
```

voice vlan (Interface)

This command is used to enable the voice vlan capability on the interface.

Syntax

```
voice vlan { vlanid | dot1p priority | none | untagged | data priority {trust |  
untrust} | auth {enable | disable} | dscp dscp}
```

no voice vlan

- *vlanid*—The voice VLAN ID.
- *priority*—The Dot1p priority for the voice VLAN on the port.

- **trust**—Trust the dot1p priority or DSCP values contained in packets arriving on the voice vlan port.
- **untrust**—Do not trust the dot1p priority or DSCP values contained in packets arriving on the voice vlan port.
- **dscp**—The DSCP value (Range: 0–64).

Default Configuration

The default DSCP value is 46.

Command Mode

Interface Configuration (Ethernet) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-1/g1)#voice vlan 1
console(config-if-1/g1)#voice vlan dot1p 1
console(config-if-1/g1)#voice vlan none
console(config-if-1/g1)#voice vlan untagged
```

voice vlan data priority

This command is to either trust or not trust (untrust) the data traffic arriving on the voice VLAN port.

Syntax

voice vlan data priority {trust | untrust}

- **trust**—Trust the dot1p priority or DSCP values contained in packets arriving on the voice vlan port.
- **untrust**—Do not trust the dot1p priority or DSCP values contained in packets arriving on the voice vlan port.

Command Mode

Interface Configuration

Default Value

trust

Example

```
console(config-if-1/g1)#voice vlan data priority untrust
```

```
console(config-if-1/g1)#voice vlan data priority trust
```

show voice vlan

```
show voice vlan [interface { <unit/port> |all}]
```

Syntax

When the **interface** parameter is not specified, only the global mode of the voice VLAN is displayed.

When the interface parameter is specified:

Voice VLAN Mode The admin mode of the voice VLAN on the interface.

Voice VLAN Id The voice VLAN ID.

Voice VLAN Priority The Dot1p priority for the voice VLAN on the port.

Voice VLAN Untagged The tagging option for the voice VLAN traffic.

Voice VLAN COS Override The Override option for the voice traffic arriving on the port.

Voice VLAN Status The operational status of voice VLAN on the port.

Command Mode

Privileged EXEC

Example

```
(console) #show voice vlan interface 1/g1
```

```
Interface.....1/g1
Voice VLAN Interface Mode.....Enabled
Voice VLAN ID.....1
Voice VLAN COS Override.....False
Voice VLAN Port Status.....Disabled
```


802.1x Commands

This chapter explains the following commands:

- `dot1x mac-auth-bypass`
- `dot1x max-req`
- `dot1x max-users`
- `dot1x port-control`
- `dot1x re-authenticate`
- `dot1x re-authentication`
- `dot1x system-auth-control`
- `dot1x timeout guest-vlan-period`
- `dot1x timeout quiet-period`
- `dot1x timeout re-authperiod`
- `dot1x timeout server-timeout`
- `dot1x timeout supp-timeout`
- `dot1x timeout tx-period`
- `show dot1x`
- `show dot1x clients`
- `show dot1x ethernet`
- `show dot1x statistics`
- `show dot1x users`

802.1x Advanced Features

- `dot1x guest-vlan`
- `dot1x unauth-vlan`
- `show dot1x advanced`

802.1x Option 81

- `radius-server attribute 4`

dot1x mac-auth-bypass

Use the **dot1x mab-enable** command to enable MAB on an interface. Use the “no” form of this command to disable MAB on an interface.

Syntax

dot1x mac-auth-bypass

no dot1x mac-auth-bypass

Default Configuration

MAC Authentication Bypass is disabled by default.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets MAC Authentication Bypass on interface 1/2:

```
console(config-if-1/g2)#dot1x mac-auth-bypass
```

dot1x max-req

Use the **dot1x max-req** command in Interface Configuration mode to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request frame (assuming that no response is received) to the client before restarting the authentication process. To return to the default setting, use the **no** form of this command.

Syntax

dot1x max-req *count*

no dot1x max-req

- *count* — Number of times that the switch sends an EAP-request/identity frame before restarting the authentication process. (Range: 1–10)

Default Configuration

The default value for the *count* parameter is 2.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the number of times that the switch sends an EAP-request/identity frame to 6.

```
console(config)# interface ethernet 1/g16
console(config-if-1/g16)# dot1x max-req 6
```

dot1x max-users

Use the **dot1x max-users** command in Interface Configuration mode to set the maximum number of clients supported on the port when MAC-based 802.1X authentication is enabled on the port. Use the **no** version of the command to reset the maximum number of clients supported on the port when MAC-based 802.1X authentication is enabled on the port. The value would be reset to 8.

Syntax

dot1x max-users *users*

no dot1x max-users

- *users* — The number of users the port supports for MAC-based 802.1X authentication (Range: 1–16)

Default Configuration

The default number of clients supported on a port with MAC-based 802.1X authentication is 8.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following command limits the number of devices that can authenticate on port 1/g2 to 3.

```
console(config-if-1/g2)#dot1x max-users 3
```

dot1x port-control

Use the **dot1x port-control** command in Interface Configuration mode to enable the IEEE 802.1X operation on the port.

Syntax

dot1x port-control {force-authorized | force-unauthorized | auto | mac-based}

no dot1x port-control

- **auto** — Enables 802.1x authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the switch and the client.
- **force-authorized** — Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port sends and receives normal traffic without 802.1x-based authentication of the client.
- **force-unauthorized** — Denies all access through this interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
- **mac-based** — Enables 802.1x authentication on the interface and allows multiple hosts to authenticate on a single port. The hosts are distinguished by their MAC addresses.

Default Configuration

The default configuration is **auto**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended that you disable the spanning tree or enable spanning-tree PortFast mode on 802.1x edge ports (ports in **auto** state that are connected to end stations), in order to go immediately to the forwarding state after successful authentication.

When configuring a port to use MAC-based authentication, the port must be in switchport general mode.

Example

The following command enables MAC-based authentication on port 1/g2

```
console(config)# interface ethernet 1/g2
```

```
console(config-if-1/g2)# dot1x port-control mac-based
```

dot1x re-authenticate

Use the **dot1x re-authenticate** command in Privileged EXEC mode to enable manually initiating a re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.

Syntax

dot1x re-authenticate [**ethernet** *interface*]

- *interface* — Specifies a valid interface number. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following command manually initiates a re-authentication of the 802.1x-enabled port.

```
console# dot1x re-authenticate ethernet 1/g16
```

dot1x re-authentication

Use the **dot1x re-authentication** command in Interface Configuration mode to enable periodic re-authentication of the client. To return to the default setting, use the **no** form of this command.

Syntax

dot1x re-authentication

no dot1x re-authentication

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables periodic re-authentication of the client.

```
console(config)# interface ethernet 1/g16
```

```
console(config-if-1/g16)# dot1x re-authentication
```

dot1x system-auth-control

Use the **dot1x system-auth-control** command in Global Configuration mode to enable 802.1x globally. To disable 802.1x globally, use the **no** form of this command.

Syntax

```
dot1x system-auth-control  
no dot1x system-auth-control
```

Default Configuration

The default for this command is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables 802.1x globally.

```
console(config)# dot1x system-auth-control
```

dot1x timeout guest-vlan-period

Use the **dot1x timeout guest-vlan-period** command in Interface Configuration mode to set the number of seconds that the switch waits before authorizing the client if the client is a dot1x unaware client.

Syntax

```
dot1x timeout guest-vlan-period seconds
```

seconds — Time in seconds that the switch waits before authorizing the client if the client is a dot1x unaware client.

Default Configuration

The switch remains in the quiet state for 90 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended that the user set the `dot1x timeout guest-vlan-period` to at least three times the `while` timer, so that at least three EAP Requests are sent, before assuming that the client is a dot1x unaware client.

Example

The following example sets the dot1x timeout guest vlan period to 100 seconds.

```
console(config)# dot1x timeout guest-vlan-period 100
```

dot1x timeout quiet-period

Use the `dot1x timeout quiet-period` command in Interface Configuration mode to set the number of seconds that the switch remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). To return to the default setting, use the `no` form of this command.

Syntax

`dot1x timeout quiet-period seconds`

`no dot1x timeout quiet-period`

- *seconds* — Time in seconds that the switch remains in the quiet state following a failed authentication exchange with the client. (Range: 0–65535 seconds)

Default Configuration

The switch remains in the quiet state for 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

During the quiet period, the switch does not accept or initiate any authentication requests.

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide a faster response time to the user, enter a smaller number than the default.

Example

The following example sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange to 3600.

```
console(config)# interface ethernet 1/g16
console(config-if-1/g16)# dot1x timeout quiet-period
3600
```

dot1x timeout re-authperiod

Use the **dot1x timeout re-authperiod** command in Interface Configuration mode to set the number of seconds between re-authentication attempts. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

- *seconds* — Number of seconds between re-authentication attempts.
(Range: 300–4294967295)

Default Configuration

Re-authentication period is 3600 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the number of seconds between re-authentication attempts to 300.

```
console(config)# interface ethernet 1/g16
console(config-if-1/g16)# dot1x timeout re-authperiod
300
```

dot1x timeout server-timeout

Use the **dot1x timeout server-timeout** command in Interface Configuration mode to set the time that the switch waits for a response from the authentication server. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

- *seconds* — Time in seconds that the switch waits for a response from the authentication server. (Range: 1–65535)

Default Configuration

The period of time is set to 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The actual timeout is this parameter or the product of the Radius transmission times the Radius timeout, whichever is smaller

Example

The following example sets the time for the retransmission to the authentication server to 3600 seconds.

```
console(config-if-1/g1)# dot1x timeout server-timeout  
3600
```

dot1x timeout supp-timeout

Use the **dot1x timeout supp-timeout** command in Interface Configuration mode to set the time that the switch waits for a response before retransmitting an Extensible Authentication Protocol (EAP)-request frame to the client. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

- *seconds* — Time in seconds that the switch should wait for a response to an EAP-request frame from the client before resending the request. (Range: 1–65535)

Default Configuration

The period of time is set to 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the time for the retransmission of an EAP-request frame to the client to 3600 seconds.

```
console(config-if-1/g1)# dot1x timeout supp-timeout  
3600
```

dot1x timeout tx-period

Use the **dot1x timeout tx-period** command in Interface Configuration mode to set the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request. To return to the default setting, use the **no** form of this command.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

- *seconds* — Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before resending the request.
(Range: 1–65535)

Default Configuration

The period of time is set to 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following command sets the number of seconds that the switch waits for a response to an EAP-request/identity frame to 3600 seconds.

```
console(config)# interface ethernet 1/g16
console(config-if-1/g16)# dot1x timeout tx-period
3600
```

show dot1x

Use the **show dot1x** command in Privileged EXEC mode to display 802.1X status for the switch or for the specified interface. This feature is an extension of Dot1x Option 81 feature added in Power Connect Release 2.1. The feature accepts a VLAN name as an alternative to a number when RADIUS indicates the Tunnel-Private-Group-ID for a supplicant.

Syntax

show dot1x [*ethernet interface*]

- *interface* — A valid Ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1X port 1/g8 status.

```
console#show dot1x ethernet 1/g8
```

```
Administrative Mode..... Disabled
```

```

Port      Admin      Oper      Reauth      Reauth
      Mode      Mode      Control      Period
-----
1/g8      auto      Authorized  FALSE      3600

User Name..... Clark
Quiet Period..... 60
Transmit Period..... 30
Maximum Requests..... 2
Max Users..... 16
VLAN Assigned.....
Supplicant Timeout..... 30
Server Timeout (secs)..... 30
Authenticator PAE State.....
Initialize
Backend Authentication State.....
Initialize
Authentication Success..... 9
Authentication Fails..... 1

```

The **show dot1x** output for a specified interface varies depending on the 802.1X Admin Mode of the port and whether any supplicants are authenticated on the port. The following table describes the significant fields shown in the display:

Field	Description
Port	The port number.
Admin mode	The port admin mode. Possible values are: Force-auth , Force-unauth , Auto , and mac-based .
Oper mode	The control mode under which this port is operating. Possible values are: Authorized or Unauthorized .

Field	Description
Reauth Control	Indicates whether re-authentication is enabled on this port.
Reauth Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Username	The username representing the identity of the Supplicant. This field shows the username when the port control is auto or mac-based . If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user that was authenticated successfully.
Quiet period	The number of seconds that the switch remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
Transmit period	The number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request.
Maximum Requests	The maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request frame (assuming that no response is received) to the client before restarting the authentication process.
Max Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode.
VLAN Assigned	The VLAN assigned to the client by the radius server. When VLAN assignments are disabled, RADIUS server does not assign any VLAN to the port, and this field is blank.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server timeout	Time in seconds the switch waits for a response from the authentication server before resending the request.

Field	Description
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
Authentication success	Counts the number of times the state machine has received a Success message from the Authentication Server.
Authentication fails	Counts the number of times the state machine has received a Failure message from the Authentication Server.
Supplicant MAC Address	The MAC-address of the supplicant
Filter-ID	The Filter Id assigned to the client by the RADIUS server. This field is not applicable when the Filter-Id feature is disabled on the RADIUS server and client.

show dot1x clients

Use the **show dot1x clients** command in Privileged EXEC mode to display detailed information about the users who have successfully authenticated on the system or on a specified port.

Syntax

show dot1x clients {all | ethernet *interface*}

- **all** — All 802.1X clients authenticated on the system
- *interface* — A valid Ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the 802.1x clients authenticated on port 1/g9.

```
console#show dot1x clients ethernet 1/g9
```

```
Interface..... 1/g9
User Name..... guest1
Supp MAC Address..... 0012.1756.76EA
Session Time..... 118
Filter Id.....
VLAN Assigned..... 1
Interface..... 1/g9
User Name..... guest1
Supp MAC Address..... 0012.1756.796B
Session Time..... 80
Filter Id.....
VLAN Assigned..... 1
```

The following table describes the significant fields shown in the display:

Field	Description
Interface	The port number.
Username	The username representing the identity of the Supplicant. This field shows the username when the port control is auto or mac-based . If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user that was authenticated successfully.
Supp MAC Address	The MAC-address of the supplicant
Session Time	The amount of time, in seconds, since the client was authenticated on the port.
Filter-ID	The Filter Id assigned to the client by the RADIUS server. This field is not applicable when the Filter-Id feature is disabled on the RADIUS server and client.
VLAN Assigned	The VLAN assigned to the client by the radius server. When VLAN assignments are disabled, RADIUS server does not assign any VLAN to the port, and this field is set to 0.

show dot1x ethernet

The **show dot1x ethernet** command has been modified to show the status of MAC Authentication Bypass. This feature is an extension of Dot1x Option 81 feature added in Power Connect Release 2.1. to accept a VLAN name as an alternative to a number when RADIUS indicates the Tunnel-Private-Group-ID for a supplicant.

Syntax

show dot1x ethernet *interface*

- *interface* — Specifies a valid interface number. The full syntax is unit/port

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

console#show dot1x ethernet 1/g1

Administrative Mode..... Disabled

Port	Admin Mode	Oper Mode	Reauth Control	Reauth Period
-----	-----	-----	-----	-----
1/g1	auto	Authorized	FALSE	3600

Quiet Period..... 60

Transmit Period..... 30

Maximum Requests..... 2

Max Users..... 16

VLAN Assigned..... 10
(exampleVlanName)

Supplicant Timeout..... 30

Server Timeout (secs)..... 30

MAB mode (configured)..... Disabled

MAB mode (operational)..... Disabled

Authenticator PAE State..... Initialize

Backend Authentication State..... Initialize

show dot1x statistics

Use the `show dot1x statistics` command in Privileged EXEC mode to display 802.1x statistics for the specified interface.

Syntax

`show dot1x statistics ethernet interface`

- *interface* — Ethernet port name. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x statistics for the specified interface.

```
console#show dot1x statistics ethernet 1/g2
```

```
Port..... 1/g2
EAPOL Frames Received..... 0
EAPOL Frames Transmitted..... 0
EAPOL Start Frames Received..... 0
EAPOL Logoff Frames Received..... 0
Last EAPOL Frame Version..... 0
Last EAPOL Frame Source..... 0000.0000.0000
EAP Response/Id Frames Received..... 0
EAP Response Frames Received..... 0
```


EAP Request/Id Frames Transmitted..... 0
EAP Request Frames Transmitted..... 0
Invalid EAPOL Frames Received..... 0
EAPOL Length Error Frames Received..... 0

The following table describes the significant fields shown in the display.

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.

Field	Description
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

show dot1x users

Use the **show dot1x users** command in Privileged EXEC mode to display 802.1x authenticated users for the switch.

Syntax

show dot1x users [*username username*]

- *username* — Supplicant username (Range: 1–160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x users.

```
console#show dot1x users
Port      Username
-----
1/g1      Bob
1/g2      John
Switch# show dot1x users username Bob
Port      Username
-----
1/g1      Bob
```

The following table describes the significant fields shown in the display:

Field	Description
Username	The username representing the identity of the Supplicant.
Port	The port that the user is using.

802.1x Advanced Features

dot1x guest-vlan

Use the `dot1x guest-vlan` command in Interface Configuration mode to set the guest VLAN on a port. The VLAN must already have been defined. The `no` form of this command sets the guest VLAN id to zero, which disables the guest VLAN on a port.

Syntax

```
dot1x guest-vlan vlan-id
```

```
no dot1x guest-vlan
```

- *vlan-id* — The ID of a valid VLAN to use as the guest VLAN (Range: 0-4093).

Default Configuration

The guest VLAN is disabled on the interface by default.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Configure the guest VLAN before using this command.

Example

The following example sets the guest VLAN on port 1/g2 to VLAN 10.

```
console(config-if-1/g2)#dot1x guest-vlan 10
```

dot1x unauth-vlan

Use the `dot1x unauth-vlan` command in Interface Configuration mode to specify the unauthenticated VLAN on a port. The unauthenticated VLAN is the VLAN to which supplicants that fail 802.1X authentication are assigned.

Syntax

```
dot1x unauth-vlan vlan-id
```

```
no dot1x unauth-vlan
```

- *vlan-id*— The ID of a valid VLAN to use for unauthenticated clients (Range: 0-4093).

Default Configuration

The unauthenticated VLAN is disabled on the interface by default.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Configure the unauthenticated VLAN before using this command.

Example

The following example set the unauthenticated VLAN on port 1/g2 to VLAN 20.

```
console (config-if-1/g2) #dot1x unauth-vlan 20
```

show dot1x advanced

Use the **show dot1x advanced** command in Privileged EXEC mode to display 802.1x advanced features for the switch or for the specified interface. The output of this command has been updated in release 2.1 to remove the Multiple Hosts column and add an Unauthenticated VLAN column, which indicates whether an unauthenticated VLAN is configured on a port. The command has also been updated to show the Guest VLAN ID (instead of the status) since it is now configurable per port.

Syntax

show dot1x advanced [*ethernet interface*]

- *interface* — Specifies a valid ethernet interface.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays 802.1x advanced features for the switch.

console#show dot1x advanced

Port	Guest	Unauthenticated
	VLAN	Vlan
-----	-----	-----
1/g1	Disabled	Disabled
1/g2	10	20
1/g3	Disabled	Disabled
1/g4	Disabled	Disabled
1/g5	Disabled	Disabled
1/g6	Disabled	Disabled

console#show dot1x advanced ethernet 1/g2

Port	Guest	Unauthenticated
	VLAN	Vlan
-----	-----	-----
1/g2	10	20

802.1x Option 81

radius-server attribute 4

Use the **radius-server attribute 4** command in Global Configuration mode to set the network access server (NAS) IP address for the RADIUS server. Use the **no** version of the command to set the value to the default.

Syntax

radius-server attribute 4 *ip-address*

no dot1x guest-vlan

- *ip-address* — Specifies the IP address to be used as the RADIUS attribute 4, the NAS IP address.

Default Configuration

If a RADIUS server has been configured on the switch, the default attribute 4 value is the RADIUS server IP address.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the NAS IP address in RADIUS attribute 4 to 192.168.10.22.

```
console(config)#radius-server attribute 4  
192.168.10.22
```


ARP Commands

This chapter explains the following commands:

- arp
- arp cachesize
- arp dynamicrenew
- arp purge
- arp resptime
- arp retries
- arp timeout
- clear arp-cache
- clear arp-cache management
- ip proxy-arp
- show arp

arp

Use the **arp** command in Global Configuration mode to create an Address Resolution Protocol (ARP) entry. Use the **no** form of the command to remove the entry.

Syntax

arp *ip-address mac-address*

no arp *ip-address*

- *ip-address* — IP address of a device on a subnet attached to an existing routing interface.
- *mac-address* — A unicast MAC address for that device.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example creates an ARP entry consisting of an IP address and a MAC address.

```
console(config)#arp 192.168.1.2 00A2.64B3.A245
```

arp cachesize

Use the **arp cachesize** command in Global Configuration mode to configure the maximum number of entries in the ARP cache. To return the maximum number ARP cache entries to the default value, use the **no** form of this command.

Syntax

`arp cachesize integer`

`no arp cachesize`

- *integer* — Maximum number of ARP entries in the cache. (Range: 256–1024)

Default Configuration

The default integer value is 896.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines an arp cachesize of 500.

```
console(config)#arp cachesize 500
```

arp dynamicrenew

Use the `arp dynamicrenew` command in Global Configuration mode to enable the ARP component to automatically renew dynamic ARP entries when they age out. To disable the automatic renewal of dynamic ARP entries when they age out, use the `no` form of the command.

Syntax

`arp dynamicrenew`

`no arp dynamicrenew`

Default Configuration

The default state is enabled.

Command Mode

Global Configuration mode

User Guidelines

When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry. If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, the system sends an ARP request to renew the entry. When an entry is not renewed, it is removed from the hardware and subsequent data packets to the host trigger an ARP request. Traffic to the host is lost until the router receives an ARP reply from the host. Gateway entries, entries for a neighbor router, are always renewed. The dynamic renew option only applies to host entries.

The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. In a network where the number of potential neighbors is greater than the ARP cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full.

Example

```
console#configure
console(config)#arp dynamicrenew
console(config)#no arp dynamicrenew
```

arp purge

Use the **arp purge** command in Privileged EXEC mode to cause the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Syntax

`arp purge ip-address`

- *ip-address* — The IP address to be removed from ARP cache.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example removes the specified IP address from arp cache.

```
console#arp purge 192.168.1.10
```

arp resptime

Use the `arp resptime` command in Global Configuration mode to configure the ARP request response timeout. To return the response timeout to the default value, use the `no` form of this command.

Syntax

`arp resptime integer`

`no arp resptime`

- *integer* — IP ARP entry response time out. (Range: 1-10 seconds)

Default Configuration

The default value is 1 second.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a response timeout of 5 seconds.

```
console(config)#arp resptime 5
```

arp retries

Use the **arp retries** command in Global Configuration mode to configure the ARP count of maximum requests for retries. To return to the default value, use the **no** form of this command.

Syntax

arp retries *integer*

no arp retries

- *integer* — The maximum number of requests for retries. (Range: 0-10)

Default Configuration

The default value is 4 retries.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines 6 as the maximum number of retries.

```
console(config)#arp retries 6
```

arp timeout

Use the **arp timeout** command in Global Configuration mode to configure the ARP entry ageout time. Use the no form of the command to set the ageout time to the default.

Syntax

arp timeout *integer*

no arp timeout

- *integer* — The IP ARP entry ageout time. (Range: 15-21600 seconds)

Default Configuration

The default value is 1200 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines 900 seconds as the timeout.

```
console(config)#arp timeout 900
```

clear arp-cache

Use the **clear arp-cache** command in Privileged EXEC mode to remove all ARP entries of type dynamic from the ARP cache.

Syntax

clear arp-cache [*gateway*]

- *gateway* — Removes the dynamic entries of type **gateway**, as well.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example clears all entries ARP of type dynamic, including gateway, from ARP cache.

```
console#clear arp-cache gateway
```

clear arp-cache management

Use the **clear arp-cache management** command to clear all entries from the ARP cache learned from the management port.

Syntax

```
clear arp-cache management
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#clear arp-cache management
```


ip proxy-arp

Use the **ip proxy-arp** command in Interface Configuration mode to enable proxy ARP on a router interface. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request. Use the **no** form of the command to disable proxy ARP on a router interface.

Syntax

ip proxy-arp

no ip proxy-arp

Default Configuration

Enabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables proxy arp for VLAN 15.

```
(config)#interface vlan 15
console(config-if-vlan15)#ip proxy-arp
```

show arp

Use the **show arp** command in Privileged EXEC mode to display the Address Resolution Protocol (ARP) cache entries statically added or dynamically learned on the routing ports. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the **show ARP** results in conjunction with the **show ARP switch** results.

Syntax

show arp [brief] [switch]

- brief — Display ARP parameters and cache.
- switch — Display ARP cache for the switch.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows **show arp** command output.

```
console#show arp
Age Time (seconds)..... 1200
Response Time (seconds)..... 1
Retries..... 4
Cache Size..... 896
Dynamic Renew Mode..... Enable
Total Entry Count Current / Peak..... 1 / 1
Static Entry Count Configured / Active / Max.. 0 / 0 / 64
```

```
console#show arp switch
```

IP Address	MAC Address	Interface	Type	Age
-----	-----	-----	-----	-----

DHCP and BOOTP Relay Commands

This chapter explains the following commands:

- `bootpdhcprelay cidridoptmode`
- `bootpdhcprelay maxhopcount`
- `bootpdhcprelay minwaittime`
- `show bootpdhcprelay`

bootpdhcrelay cidridoptmode

Use the **bootpdhcrelay cidridoptmode** command in Global Configuration mode to enable the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the system. Use the no form of the command to disable the circuit ID option and remote agent ID mode for BootP/DHCP Relay.

Syntax

bootpdhcrelay cidridoptmode arpshow arpw arpoptshshow arposhow
arpwshow arp arpshoshow arpw arpshow arpmshow arpode

Default Configuration

Disabled is the default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the circuit ID and remote agent ID options.

```
console(config)#bootpdhcrelay ?
```

```
cidridoptmode..... Enable/Disable Circuit Id Option and  
Remote Agent Id
```

```
Mode.
```

```
maxhopcount..... Configure the maximum hop count.
```

```
minwaittime..... Configure the minimum wait time.
```

The range of valid values for **maxhopcount** is 1-16. The range of valid values for **minwaittime** is 0-100 seconds.

bootpdhcprelay maxhopcount

Use the **bootpdhcprelay maxhopcount** command in Global Configuration mode to configure the maximum allowable relay agent hops for BootP/DHCP Relay on the system. Use the no form of the command to set the maximum hop count to the default value.

Syntax

bootpdhcprelay maxhopcount *integer*

no bootpdhcprelay maxshshow arpshow arpw arpopcshow arpsshshow show arppow arphshow arpow show arparpoint

- *integer*— Maximum allowable relay agent hops for BootP/DHCP Relay on the system. (Range: 1-16)

Default Configuration

The default *integer* configuration is 4.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a maximum hopcount of 6.

```
console(config)#bootpdhcprelay maxhopcount 6
```

bootpdhcprelay minwaittime

Use the **bootpdhcprelay minwaittime** command in Global Configuration mode to configure the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it might use the seconds-sinceclient- began-booting field of the request as a factor in deciding whether to relay the request or not. Use the no form of the command to set the minimum wait time to the default value.

Syntax

`bootpdhcprelay minwaittime integer`

`no bootpdhcprelay minshoshow arpshow arpwshshow arposhow
arpwshoshow arpwshow arp arp ashow arprwaittime`

- *integer* — Minimum wait time for BootP/DHCP Relay on the system.
(Range: 0-100 seconds)

Default Configuration

0 is the default *integer* configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a minimum wait time of 10 seconds.

```
console(config)#bootpdhcprelay minwaittime 10
```

bootpdhcprelay cidridoptmode

Use the `bootpdhcprelay cidridoptmode` command in Global Configuration mode to enable the circuit ID option and remote agent ID mode for BootP/DHCP Relay on the system. Use the "no" form of the command to disable the circuit ID option and remote agent ID mode for BootP/DHCP Relay.

Syntax

`bootpdhcprelay cidridoptmode arpshow arpw arpoptshshow arposhow
arpwshow arp arposhshow arpw arpshow arpmshow arpode`

Default Configuration

Disabled is the default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the circuit ID and remote agent ID options.

```
console(config)#bootpdhcprelay cidridoptmode
```

Circuit Id and Remote Agent Id Mode set Successfully.

show bootpdhcprelay

Use the **show bootpdhcprelay** command in User EXEC mode to display the BootP/DHCP Relay information.

Syntax

```
show bootpdhcprelay
```

Default Configuration

The command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example defines the Boot/DHCP Relay information.

```
console#show bootpdhcprelay
```

```
Maximum Hop Count..... 4
Minimum Wait Time(Seconds)..... 0
Circuit Id Option Mode.....
Disable
```


DHCPv6 Commands

This chapter explains the following commands:

- `clear ipv6 dhcp`
- `dns-server`
- `domain-name`
- `ipv6 dhcp pool`
- `ipv6 dhcp relay`
- `ipv6 dhcp relay-agent-info-opt`
- `ipv6 dhcp relay-agent-info-remote-id-subopt`
- `ipv6 dhcp server`
- `prefix-delegation`
- `service dhcpv6`
- `show ipv6 dhcp`
- `show ipv6 dhcp binding`
- `show ipv6 dhcp interface`
- `show ipv6 dhcp pool`
- `show ipv6 dhcp statistics`

clear ipv6 dhcp

Use the `clear ipv6 dhcp` command in Privileged EXEC mode to clear DHCPv6 statistics for all interfaces or for a specific interface.

Syntax

`clear ipv6 dhcp {statistics | interface vlan vlan-id statistics}`

- *vlan-id* — Valid VLAN ID.
- `statistics` — Indicates statistics display if VLAN is specified.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples clear DHCPv6 statistics for VLAN 11.

```
console#clear ipv6 dhcp interface vlan 11 statistics
```

dns-server

Use the `dns-server` command in IPv6 DHCP Pool Configuration mode to set the ipv6 DNS server address which is provided to a DHCPv6 client by the DHCPv6 server. DNS server address is configured for stateless server support.

Syntax

`dns-server dns-server-address`

`no dns-server dns-server-address`

- *dns-server-address* — Valid IPv6 address.

Default Configuration

This command has no default configuration.

Command Mode

IPv6 DHCP Pool Configuration mode

User Guidelines

DHCPv6 pool can have multiple number of domain names with maximum of 8.

Example

The following example sets the ipv6 DNS server address of 2020:1::1, which is provided to a DHCPv6 client by the DHCPv6 server.

```
console(config)#ipv6 dhcp pool addrpool
console(config-dhcp6s-pool)#dns-server 2020:1::1
```

domain-name

Use the **domain-name** command in IPv6 DHCP Pool Configuration mode to set the DNS domain name which is provided to a DHCPv6 client by the DHCPv6 server. DNS domain name is configured for stateless server support.

Syntax

domain-name *dns-domain-name*

no domain-name *dns-domain-name*

- *dns-domain-name* — DHCPv6 domain name. (Range: 1–255 characters)

Default Configuration

This command has no default configuration.

Command Mode

IPv6 DHCP Pool Configuration mode

User Guidelines

DHCPv6 pool can have multiple number of domain names with maximum of 8.

Example

The following example sets the DNS domain name "test", which is provided to a DHCPv6 client by the DHCPv6 server.

```
console(config)#ipv6 dhcp pool addrpool
console(config-dhcp6s-pool)#domain-name test
console(config-dhcp6s-pool)#no domain-name test
```

ipv6 dhcp pool

Use the **ipv6 dhcp pool** command in Global Configuration mode to enter IPv6 DHCP Pool Configuration mode. DHCPv6 pools are used to specify information for DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

Syntax

ipv6 dhcp pool *pool-name*

no ipv6 dhcp pool *pool-name*

- *pool-name* — DHCPv6 pool name. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters IPv6 DHCP Pool Configuration mode.

```
console(config)#ipv6 dhcp pool addrpool
console(config-dhcp6s-pool)#
```

ipv6 dhcp relay

Use the **ipv6 dhcp relay** command in Interface Configuration mode to configure an interface for DHCPv6 relay functionality.

Syntax

ipv6 dhcp relay {*destination relay-address* [**interface** **vlan** *vlan-id*] | **interface** **vlan** *vlan-id*} [**remote-id** {**duid-ifid** | *user-defined-string*}]

- **destination** — Keyword that sets the relay server IPv6 address.
- *relay-address* — An IPv6 address of a DHCPv6 relay server.
- **interface** — Sets the relay server interface.
- *vlan-id* — A valid VLAN ID.
- [**remote-id** {**duid-ifid** | *user-defined-string*}] — The Relay Agent Information Option “remote ID” sub-option to be added to relayed messages. This can either be the special keyword **duid-ifid**, which causes the “remote ID” to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel) mode

User Guidelines

If *relay-address* is an IPv6 global address, then *relay-interface* is not required. If *relay-address* is a link-local or multicast address, then *relay-interface* is required. Finally, a value for *relay-address* is not specified, then a value for *relay-interface* must be specified and the DHCPV6-ALLAGENTS multicast address (i.e. FF02::1:2) is used to relay DHCPv6 messages to the relay server.

Example

The following example configures VLAN 15 for DHCPv6 relay functionality.

```
console(config)#interface vlan 15

console(config-if-vlan15)#ipv6 dhcp relay destination
2020:1::1
```

ipv6 dhcp relay-agent-info-opt

Use **ipv6 dhcp relay-agent-info-opt** command in Global Configuration mode to configure a number to represent the DHCPv6 Relay Agent Information Option. The DHCPv6 Relay Agent Information Option allows for various sub-options to be attached to messages that are being relayed by the local router to a relay server. The relay server may in turn use this information in determining an address to assign to a DHCPv6 client.

Syntax

ipv6 dhcp relay-agent-info-opt *option*

- *option* — Agent information option. (Range: 54-65535)

Default Configuration

The default value for *option* is 54.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the number 100 to represent the DHCPv6 Relay Agent Information Option.

```
console(config)#ipv6 dhcp relay-agent-info-opt 100
```

ipv6 dhcp relay-agent-info-remote-id-subopt

Use the `ipv6 dhcp relay-agent-info-remote-id-subopt` command in Global Configuration mode to configure a number to represent the DHCPv6 the “remote-id” sub-option.

Syntax

`ipv6 dhcp relay-agent-info-remote-id-subopt suboption`

- *suboption* — Remote ID suboption. (Range: 1-65535)

Default Configuration

The default value for *suboption* is 1.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the number 100 to represent the DHCPv6 the “remote-id” sub-option.

```
console(config)#ipv6 dhcp relay-agent-info-remote-id-subopt 100
```

ipv6 dhcp server

Use the `ipv6 dhcp server` command in Interface Configuration mode to configure DHCPv6 server functionality on an interface. For a particular interface DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

Syntax

`ipv6 dhcp server pool-name [rapid-commit] [preference pref-value]`

- *pool-name* — The name of the DHCPv6 pool containing stateless and/or prefix delegation parameters
- **rapid-commit** — Is an option that allows for an abbreviated exchange between the client and server.
- *pref-value* — Preference value—used by clients to determine preference between multiple DHCPv6 servers. (Range: 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures DHCPv6 server functionality.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ipv6 dhcp server pool
```

prefix-delegation

Use the **prefix-delegation** command in IPv6 DHCP Pool Configuration mode to define Multiple IPv6 prefixes within a pool for distributing to specific DHCPv6 Prefix delegation clients.

Syntax

`prefix-delegation prefix/prefixlength DUID [name hostname] [preferred-lifetime {infinite | preferred-lifetime}]`

`no prefix-delegation prefix/prefixlength`

- *prefix/prefixlength* — Delegated IPv6 prefix.

- *DUID* — Client DUID (e.g. 00:01:00:09:f8:79:4e:00:04:76:73:43:76').
- *hostname* — Client hostname used for logging and tracing. (Range: 0-31 characters.)
- *valid-lifetime* — Valid lifetime for delegated prefix. (Range: 0-4294967295 seconds)
- *preferred-lifetime* — Preferred lifetime for delegated prefix. (Range: 0-4294967295 seconds)

Default Configuration

2592000 seconds is the default value for *preferred-lifetime*. 604800 seconds is the default value for *valid-lifetime*.

Command Mode

IPv6 DHCP Pool Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a Multiple IPv6 prefix and client DUID within a pool for distributing to specific DHCPv6 Prefix delegation clients.

```
console(config)#ipv6 dhcp pool addrpool
console(config-dhcp6s-pool)#prefix-delegation
2020:1::1/64 00:01:00:09:f8:79:4e:00:04:76:73:43:76
```

service dhcpv6

Use the **service dhcpv6** command in Global Configuration mode to enable DHCPv6 configuration on the router.

Syntax

```
service dhcpv6
no service dhcpv6
```

Default Configuration

Enabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables DHCPv6 globally.

```
console#configure
```

```
console(config)#service dhcpv6
```

```
console(config)#no service dhcpv6
```

show ipv6 dhcp

Use the `show ipv6 dhcp` command in Privileged EXEC mode to display the DHCPv6 server name and status.

Syntax

```
show ipv6 dhcp
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the DHCPv6 server name and status.

```
console#show ipv6 dhcp
```

```
DHCPv6 is disabled
```

```
Server DUID:
```

show ipv6 dhcp binding

Use the **show ipv6 dhcp binding** command in Privileged EXEC mode to display the configured DHCP pool.

Syntax

```
show ipv6 dhcp binding [ipv6-addr]
```

- *ipv6-addr* — Valid IPv6 address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the configured DHCP pool based on the entered IPv6 address.

```
console#show ipv6 dhcp binding 2020:1::
```

show ipv6 dhcp interface

Use the `show ipv6 dhcp interface` command in User EXEC mode to display DHCPv6 information for all relevant interfaces or a specified interface. If an interface is specified, the optional statistics parameter is available to view statistics for the specified interface.

Syntax

`show ipv6 dhcp interface {tunnel tunnel-id | vlan vlan-id} [statistics]`

- *tunnel-id* — Tunnel identifier. (Range: 0–7)
- *vlan-id* — Valid VLAN ID.
- *statistics* — Enables statistics display if interface is specified.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display DHCPv6 information for VLAN 11.

```
console> show ipv6 dhcp interface vlan 11
```

```
IPv6 Interface.....  
vlan11
```

```
Mode..... Relay
```

```
Relay Address.....  
2020:1::1
```

```
Relay Interface Number..... Relay
```

```
Relay Remote ID.....
```

Option Flags.....

console> show ipv6 dhcp interface vlan 11 statistics

DHCPv6 Interface vlan11 Statistics

```
-----
DHCPv6 Solicit Packets Received..... 0
DHCPv6 Request Packets Received..... 0
DHCPv6 Confirm Packets Received..... 0
DHCPv6 Renew Packets Received..... 0
DHCPv6 Rebind Packets Received..... 0
DHCPv6 Release Packets Received..... 0
DHCPv6 Decline Packets Received..... 0
DHCPv6 Inform Packets Received..... 0
DHCPv6 Relay-forward Packets Received..... 0
DHCPv6 Relay-reply Packets Received..... 0
DHCPv6 Malformed Packets Received..... 0
Received DHCPv6 Packets Discarded..... 0
Total DHCPv6 Packets Received..... 0
DHCPv6 Advertisement Packets Transmitted..... 0
DHCPv6 Reply Packets Transmitted..... 0
DHCPv6 Reconfig Packets Transmitted..... 0
DHCPv6 Relay-reply Packets Transmitted..... 0
DHCPv6 Relay-forward Packets Transmitted..... 0
Total DHCPv6 Packets Transmitted..... 0
```

show ipv6 dhcp pool

Use the `show ipv6 dhcp pool` command in Privileged EXEC mode to display the configured DHCP pool.

Syntax

`show ipv6 dhcp pool pool-name`

- *pool-name* — Name of the pool. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the configured DHCP pool.

```
console#show ipv6 dhcp pool test
```

```
DHCPv6 Pool: test
```

show ipv6 dhcp statistics

Use the `show ipv6 dhcp statistics` command in User EXEC mode to display the DHCPv6 server name and status.

Syntax

`show ipv6 dhcp statistics`

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the DHCPv6 server name and status.

```
console> show ipv6 dhcp statistics
```

```
DHCPv6 Interface Global Statistics
```

```
-----  
DHCPv6 Solicit Packets Received..... 0  
DHCPv6 Request Packets Received..... 0  
DHCPv6 Confirm Packets Received..... 0  
DHCPv6 Renew Packets Received..... 0  
DHCPv6 Rebind Packets Received..... 0  
DHCPv6 Release Packets Received..... 0  
DHCPv6 Decline Packets Received..... 0  
DHCPv6 Inform Packets Received..... 0  
DHCPv6 Relay-forward Packets Received..... 0  
DHCPv6 Relay-reply Packets Received..... 0  
DHCPv6 Malformed Packets Received..... 0  
Received DHCPv6 Packets Discarded..... 0  
Total DHCPv6 Packets Received..... 0  
DHCPv6 Advertisement Packets Transmitted..... 0  
DHCPv6 Reply Packets Transmitted..... 0  
DHCPv6 Reconfig Packets Transmitted..... 0  
DHCPv6 Relay-reply Packets Transmitted..... 0
```

```
DHCPv6 Relay-forward Packets Transmitted..... 0
Total DHCPv6 Packets Transmitted..... 0
```


DVMRP Commands

This chapter explains the following commands:

- `ip dvmrp`
- `ip dvmrp metric`
- `ip dvmrp trapflags`
- `show ip dvmrp`
- `show ip dvmrp interface`
- `show ip dvmrp neighbor`
- `show ip dvmrp nexthop`
- `show ip dvmrp prune`
- `show ip dvmrp route`

ip dvmrp

Use the **ip dvmrp** command to set the administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

Syntax

ip dvmrp

no ip dvmrp

Default Configuration

Disabled is the default configuration.

Command Mode

Global Configuration

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets VLAN 15's administrative mode of DVMRP to active.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip dvmrp
```

ip dvmrp metric

Use the **ip dvmrp metric** command in Interface Configuration mode to configure the metric for an interface. This value is used in the DVMRP messages as the cost to reach this network.

Syntax

ip dvmrp metric *metric*

no ip dvmrp metric

- *metric* — Cost to reach the network. (Range: 1-31)

Default Configuration

1 the default value.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a metric of 5 for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip dvmrp metric 5
```

ip dvmrp trapflags

Use the **ip dvmrp trapflags** command in Global Configuration mode to enable the DVMRP trap mode.

Syntax

```
ip dvmrp trapflags
no ip dvmrp trapflags
```

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following command enables DVMRP trap mode.

```
console#configure
```

```
console(config)#ip dvmrp trapflags
console(config)#no ip dvmrp trapflags
```

show ip dvmrp

Use the `show ip dvmrp` command in Privileged EXEC mode to display the system-wide information for DVMRP.

Syntax

```
show ip dvmrp
```

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays system-wide information for DVMRP.

```
console(config)#show ip dvmrp
Admin Mode..... Disable
Version..... 3
Total Number of Routes..... 0
Reachable Routes..... 0

          DVMRP INTERFACE STATUS

Interface  Interface Mode  Protocol State
-----  -
```

show ip dvmrp interface

Use the **show ip dvmrp interface** command in Privileged EXEC mode to display the interface information for DVMRP on the specified interface.

Syntax

show ip dvmrp interface *vlan vlan-id*

- *vlan-id*— Valid VLAN ID.

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays interface information for VLAN 11 DVMRP.

```
console(config)#show ip dvmrp interface vlan 11
```

```
Interface Mode..... Disable
```

show ip dvmrp neighbor

Use the **show ip dvmrp neighbor** command in Privileged EXEC mode to display the neighbor information for DVMRP.

Syntax

show ip dvmrp neighbor

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the neighbor information for DVMRP.

```
console(config)#show ip dvmrp neighbor
```

```
No neighbors available.
```

show ip dvmrp nexthop

Use the **show ip dvmrp nexthop** command in Privileged EXEC mode to display the next hop information on outgoing interfaces for routing multicast datagrams.

Syntax

```
show ip dvmrp nexthop
```

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the next hop information on outgoing interfaces for routing multicast datagrams.

```
console(config)#show ip dvmrp nexthop
```

		Next Hop	
Source IP	Source Mask	Interface	Type
-----	-----	-----	-----

show ip dvmrp prune

Use the `show ip dvmrp prune` command in Privileged EXEC mode to display the table that lists the router’s upstream prune information.

Syntax

```
show ip dvmrp prune
```

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the table that lists the router’s upstream prune information.

```
console(config)#show ip dvmrp prune
```

Group	IP Source	IP Source Mask	Expiry Time(secs)
-----	-----	-----	-----

show ip dvmrp route

Use the `show ip dvmrp route` command in Privileged EXEC mode to display the multicast routing information for DVMRP.

Syntax

`show ip dvmrp route`

Default Configuration

This command has no default condition.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the multicast routing information for DVMRP.

```
console#show ip dvmrp route

                Upstream                Expiry      Up Time
Source Address Neighbor Interface Metric Time(secs) (secs)
-----
-----
```


IGMP Commands

This chapter explains the following commands:

- ip igmp
- ip igmp last-member-query-count
- ip igmp last-member-query-interval
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp robustness
- ip igmp startup-query-count
- ip igmp startup-query-interval
- ip igmp version
- show ip igmp
- show ip igmp groups
- show ip igmp interface
- show ip igmp interface membership
- show ip igmp interface stats

ip igmp

Use the **ip igmp** command in Global Configuration mode to set the administrative mode of IGMP in the system to active.

Syntax

ip igmp

no ip igmp

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example globally enables IGMP.

```
console(config)#ip igmp
```

ip igmp last-member-query-count

Use the **ip igmp last-member-query-count** command in Interface Configuration mode to set the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface.

Syntax

ip igmp last-member-query-count *count*

no ip igmp last-member-query-count

- *count* — Query count. (Range: 1-20)

Default Configuration

The default last member query count is 2.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets 10 as the number of VLAN 2 Group-Specific Queries.

```
console#configure
console(config)#interface vlan 2
console(config-if-vlan2)#ip igmp last-member-query-
count 10
console(config-if-vlan2)#no ip igmp last-member-
query-count
```

ip igmp last-member-query-interval

Use the **ip igmp last-member-query-interval** command in Interface Configuration mode to configure the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages.

Syntax

ip igmp last-member-query-interval *tenths of seconds*

no ip igmp last-member-query-interval

- *tenths of seconds* — Maximum Response Time in tenths of a second (Range: 0-255)

Default Configuration

The default Maximum Response Time value is ten (in tenths of a second).

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures 2 seconds as the Maximum Response Time inserted in VLAN 15's Group-Specific Queries.

```
console(config)#interface vlan 15  
  
console(config-if-vlan15)#ip igmp last-member-query-  
interval 20
```

ip igmp query-interval

Use the **ip igmp query-interval** command in Interface Configuration mode to configure the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval

- *seconds* — Query interval. (Range: 1-3600)

Default Configuration

The default query interval value is 125 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a 10-second query interval for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip igmp query-interval 10
```

ip igmp query-max-response-time

Use the **ip igmp query-max-response-time** command in Internet Configuration mode to configure the maximum response time interval for the specified interface. It is the maximum query response time advertised in ICMPv2 queries on this interface. The time interval is specified in tenths of a second.

Syntax

ip igmp query-max-response-time *tenths of seconds*

no ip igmp query-max-response-time

- *tenths of seconds* — Maximum response time. (Range: 1-25 seconds)

Default Configuration

The default maximum response time value is 100 tenths of seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a maximum response time interval of one second for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip igmp query-max-response-time 10
```

ip igmp robustness

Use the **ip igmp robustness** command in Interface Configuration mode to configure the robustness that allows tuning of the interface, that is, tuning for the expected packet loss on a subnet. If a subnet is expected to have significant loss, the robustness variable may be increased for the interface.

Syntax

ip igmp robustness *robustness*

no ip igmp robustness

- *robustness* — Robustness variable. (Range: 1-255)

Default Configuration

The default robustness value is 2.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures a robustness value of 10 for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip igmp robustness 10
```

ip igmp startup-query-count

Use the **ip igmp startup-query-count** command in Interface Configuration mode to set the number of queries sent out on startup—at intervals equal to the startup query interval for the interface.

Syntax

ip igmp startup-query-count *count*

no ip igmp startup-query-count

- *count* — The number of startup queries. (Range: 1-20)

Default Configuration

The default count value is 2.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets for VLAN 15 the number of queries sent out on startup at 10.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp startup-query-count
10
```

ip igmp startup-query-interval

Use the **ip igmp startup-query-interval** command in Interface Configuration mode to set the interval between general queries sent at startup on the interface.

Syntax

ip igmp startup-query-interval *seconds*

no ip igmp startup-query-interval

- *seconds* — Startup query interval. (Range: 1-300 seconds)

Default Configuration

The default interval value is 31 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets at 10 seconds the interval between general queries sent at startup for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip igmp startup-query-  
interval 10
```

ip igmp version

Use the **ip igmp version** command in Interface Configuration mode to configure the version of IGMP for an interface.

Syntax

```
ip igmp version version
```

- *version* — IGMP version. (Range: 1-3)

Default Configuration

The default version is 3.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example configures version 2 of IGMP for VLAN 15.

```
console#interface vlan 15
```



```
console(config-if-vlan15)#ip igmp version 2
```

show ip igmp

Use the **show ip igmp** command in Privileged EXEC mode to display system-wide IGMP information.

Syntax

```
show ip igmp
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays system-wide IGMP information.

```
console#show ip igmp
```

```
IGMP Admin Mode..... Enabled
IGMP Router-Alert check..... Disabled
```

IGMP INTERFACE STATUS

```
Interface Interface-Mode Operational-Status
```

```
-----
```

```
vlan 3      Enabled      Non-Operational
```

show ip igmp groups

Use the `show ip igmp groups` command in Privileged EXEC mode to display the registered multicast groups on the interface. If **detail** is specified, this command displays the registered multicast groups on the interface in detail.

Syntax

`show ip igmp groups interface vlan vlanid [detail]`

- *vlan-id* — Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the registered multicast groups for VLAN 1.

```
console#show ip igmp groups interface vlan 3 detail
```

REGISTERED MULTICAST GROUP DETAILS						
			Version1		Version2	
Group			Host	Host	Compat	
Multicast	Last Up	Expiry	Host	Host	Timer	Timer
IP Address	Reporter	Time	Time	Timer	Timer	Mode
-----	-----	-----	-----	-----	-----	-----
225.0.0.5	1.1.1.5	00:00:05	00:04:15	-----		
00:04:15 v2						

show ip igmp interface

Use the **show ip igmp interface** command in Privileged EXEC mode to display the IGMP information for the specified interface.

Syntax

show ip igmp interface *vlan* *vlan-id*

- *vlan-id*— Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IGMP information for VLAN 11.

```
console#show ip igmp vlan 11
Interface..... 11
IGMP Admin Mode..... Enable
Interface Mode.....Enable
IGMP Version..... 3
Query Interval (secs)..... 125
Query Max Response Time (1/10 of a second)..... 100
Robustness..... 2
Startup Query Interval (secs)..... 31
Startup Query Count..... 2
Last Member Query Interval (1/10 of a second)...10
Last Member Query Count..... 2
```

show ip igmp interface membership

Use the `show ip igmp interface membership` command in Privileged EXEC mode to display the list of interfaces that have registered in the multicast group. If `detail` is specified, this command displays detailed information about the listed interfaces.

Syntax

`show ip igmp interface membership groupaddr [detail]`

- groupaddr* — Group IP address

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display the list of interfaces that have registered in the multicast group at IP address 224.5.5.5, the latter in detail mode.

```
console#show ip igmp interface membership 224.5.5.5
IGMP INTERFACE MEMBERSHIP INFO
Interface  Interface IP      State      Group Compat Source Filter
                                     Mode        Mode
-----
-----

console(config)#show ip igmp interface membership 224.5.5.5 detail
IGMP INTERFACE DETAILED MEMBERSHIP INFO
Interface  Group Compat  Source Filter  Source Hosts  Expiry Time
          Mode           Mode
-----
-----
-
```

show ip igmp interface stats

Use the `show ip igmp interface stats` command in User EXEC mode to display the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

Syntax

`show ip igmp interface stats vlan vlan-id`

- *vlan-id* — Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

This command has no user guidelines.

Examples

The following example displays the IGMP statistical information for VLAN 7.

```
console#show ip igmp interface stats vlan 7
Querier Status.....
Querier
Querier IP Address.....
7.7.7.7
Querier Up Time (secs)..... 55372
Querier Expiry Time (secs)..... 0
Wrong Version Queries..... 0
Number of Joins..... 7
Number of Groups..... 1
```


IGMP Proxy Commands

This chapter explains the following commands:

- `ip igmp-proxy`
- `ip igmp-proxy reset-status`
- `ip igmp-proxy unsolicited-report-interval`
- `show ip igmp-proxy`
- `show ip igmp-proxy interface`
- `show ip igmp-proxy groups`
- `show ip igmp-proxy groups detail`

ip igmp-proxy

Use the **ip igmp-proxy** command in Interface Configuration mode to enable the IGMP Proxy on the router. To enable the IGMP Proxy on the router, multicast forwarding must be enabled and there must be no multicast routing protocols enabled on the router.

Syntax

```
ip igmp-proxy  
no ip igmp-proxy
```

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the IGMP Proxy on the VLAN 15 router.

```
console(config)#interface vlan 15  
console(config-if-vlan15)#ip igmp-proxy
```

ip igmp-proxy reset-status

Use the **ip igmp-proxy reset-status** command in Interface Configuration mode to reset the host interface status parameters of the IGMP Proxy router. This command is valid only when IGMP Proxy is enabled on the interface.

Syntax

```
ip igmp-proxy reset-status
```


Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example resets the host interface status parameters of the IGMP Proxy router.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp-proxy reset-status
```

ip igmp-proxy unsolicited-report-interval

Use the **ip igmp-proxy unsolicited-report-interval** command in Interface Configuration mode to set the unsolicited report interval for the IGMP Proxy router. This command is valid only if IGMP Proxy on the interface is enabled.

Syntax

ip igmp-proxy unsolicited-report-interval *seconds*

- *seconds* — Unsolicited report interval. (Range: 1-260 seconds)

Default Configuration

The default configuration is 1 second.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets 10 seconds as the unsolicited report interval for the IGMP Proxy router.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip igmp-proxy unsolicited-
report-interval 10
```

show ip igmp-proxy

Use the **show ip igmp-proxy** command in Privileged EXEC mode to display a summary of the host interface status parameters. It displays status parameters only when IGMP Proxy is enabled.

Syntax

```
show ip igmp-proxy
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary of the host interface status parameters.

```
console#show ip igmp-proxy

Interface Index.....
vlan13

Admin Mode.....
Enable
```

```
Operational Mode..... Enable
Version..... 3
Number of Multicast Groups..... 0
Unsolicited Report Interval..... 1
Querier IP Address on Proxy Interface..... 0.0.0.0
Older Version 1 Querier Timeout..... 0
Older Version 2 Querier Timeout..... 0
Proxy Start Frequency..... 1
```

show ip igmp-proxy interface

Use the `show ip igmp-proxy interface` command in Privileged EXEC mode to display a detailed list of the host interface status parameters. It displays status parameters only when IGMP Proxy is enabled.

Syntax

`show ip igmp-proxy interface`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example fails to display status parameters because IGMP Proxy is not enabled.

```
console#show ip igmp-proxy interface
Interface Index..... vlan13
Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
```

1	0	0	0	-----	-----
2	0	0	0	0	0
3	0	0	0	-----	-----

show ip igmp-proxy groups

Use the **show ip igmp-proxy groups** command in Privileged EXEC mode to display a table of information about multicast groups that IGMP Proxy reported. It displays status parameters only when IGMP Proxy is enabled.

Syntax

show ip igmp-proxy groups

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example attempts to display a table of information about multicast groups that IGMP Proxy reported.

```

console#show ip igmp-proxy groups
Interface Index..... vlan13
Group Address  Last Reporter    Up Time    Member State Filter
Mode Sources
-----
225.0.1.1      13.13.13.1      7          DELAY-
MEMBER Exclude      0
225.0.1.2      13.13.13.1      48         DELAY-
MEMBER Exclude      0

```

show ip igmp-proxy groups detail

Use the `show ip igmp-proxy groups detail` command in Privileged EXEC mode to display complete information about multicast groups that IGMP Proxy has reported.

Syntax

`show ip igmp-proxy groups detail`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays complete information about multicast groups that IGMP Proxy has reported.

```
console#show ip igmp-proxy groups detail
Interface Index..... vlan13
Group Address  Last Reporter    Up Time   Member State Filter
Mode Sources
-----
-----
225.0.1.1      13.13.13.1      26        DELAY-
MEMBER Exclude 0
225.0.1.2      13.13.13.1      67        DELAY-
MEMBER Exclude 0
```


IP Helper Commands

This chapter explains the following commands:

- clear ip helper statistics
- ip helper-address (global configuration)
- ip helper-address (interface configuration)
- ip helper enable
- show ip helper-address
- show ip helper statistics

clear ip helper statistics

Use the `clear ip helper statistics` command to reset to 0 the statistics displayed in `show ip helper statistics`.

Syntax

`clear ip helper statistics`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#clear ip helper statistics
```

ip helper-address (global configuration)

Use the `ip helper-address (global configuration)` command to configure the relay of certain UDP broadcast packets received on any interface. To delete an IP helper entry, use the `no` form of this command.

Syntax

`ip helper-address server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

`no ip helper-address [server-address] [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

- *server-address* — The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.

- *dest-udp-port* — A destination UDP port number from 0 to 65535.
- *port-name* — The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: **dhcp** (port 67), **domain** (port 53), **isakmp** (port 500), **mobile-ip** (port 434), **nameserver** (port 42), **netbios-dgm** (port 138), **netbios-ns** (port 137), **ntp** (port 123), **pim-auto-rp** (port 496), **rip** (port 520), **tacacs** (port 49), **tftp** (port 69), and **time** (port 37). Other ports must be specified by number.

Default Configuration

No helper addresses are configured.

Command Mode

Global Configuration mode.

User Guidelines

This command can be invoked multiple times, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

The command `no ip helper-address` with no arguments clears all global IP helper addresses.

Example

To relay DHCP packets received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1, use the following commands:

```
console#config
console(config)#ip helper-address 10.1.1.1 dhcp
console(config)#ip helper-address 10.1.2.1 dhcp
```

To relay UDP packets received on any interface for all default ports (Table 4) to the server at 20.1.1.1, use the following commands:

```
console#config
```

```
console(config)#ip helper-address 20.1.1.1
```

ip helper-address (interface configuration)

Use the **ip helper-address (interface configuration)** command to configure the relay of certain UDP broadcast packets received on a specific interface. To delete a relay entry on an interface, use the **no** form of this command.

Syntax

```
ip helper-address {server-address | discard} [dest-udp-port | dhcp | domain  
| isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-  
auto-rp | rip | tacacs | tftp | time]
```

```
no ip helper-address [server-address | discard] [dest-udp-port | dhcp |  
domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp  
| pim-auto-rp | rip | tacacs | tftp | time]
```

- *server-address* — The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
- **discard** — Matching packets should be discarded rather than relayed, even if a global ip helper-address configuration matches the packet.
- *dest-udp-port* — A destination UDP port number from 0 to 65535.
- *port-name* — The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: **dhcp** (port 67), **domain** (port 53), **isakmp** (port 500), **mobile-ip** (port 434), **nameserver** (port 42), **netbios-dgm** (port 138), **netbios-ns** (port 137), **ntp** (port 123), **pim-auto-rp** (port 496), **rip** (port 520), **tacacs** (port 49), **tftp** (port 69), and **time** (port 37). Other ports must be specified by number.

Default Configuration

No helper addresses are configured.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command can be invoked multiple times on routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

The command `no ip helper-address` with no arguments clears all helper addresses on the interface.

Example

To relay DHCP packets received on vlan 5 to two DHCP servers, 192.168.10.1 and 192.168.20.1, use the following commands:

```
console#config
console(config)#interface vlan 5
console(config-if-vlan5)#ip helper-address
192.168.10.1 dhcp
console(config-if-vlan5)#ip helper-address
192.168.20.1 dhcp
```

To relay both DHCP and DNS packets to 192.168.30.1, use the following commands:

```
console#config
console(config)#interface vlan 5
console(config-if-vlan5)#ip helper-address
192.168.30.1 dhcp
console(config-if-vlan5)#ip helper-address
192.168.30.1 dns
```

This command takes precedence over an `ip helper-address` command given in global configuration mode. With the following configuration, the relay agent relays DHCP packets received on any interface other than vlan 5 and vlan 6 to 192.168.40.1, relays DHCP and DNS packets received on vlan 5 to 192.168.40.2, relays SNMP traps (port 162) received on interface vlan 6 to 192.168.23.1, and drops DHCP packets received on vlan 6:

```
console#config
console(config)#ip helper-address 192.168.40.1 dhcp
console(config)#interface vlan 5
console(config-if-vlan5)#ip helper-address
192.168.40.2 dhcp
console(config-if-vlan5)#ip helper-address
192.168.40.2 domain
console(config-if-vlan5)#exit
console(config)#interface 2/6
console(config-if-vlan6)#ip helper-address
192.168.23.1 162
console(config-if-vlan6)#ip helper-address discard
dhcp
```

ip helper enable

Use the `ip helper enable` command to enable relay of UDP packets. To disable relay of all UDP packets, use the “no” form of this command.

Syntax

```
ip helper enable
no ip helper enable
```

Default Configuration

IP helper is enabled by default.

Command Mode

Global Configuration mode.

User Guidelines

This command can be used to temporarily disable IP helper without deleting all IP helper addresses.

This command replaces the `bootpdhcprelay enable` command, but affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.

Example

```
console(config)#ip helper enable
```

show ip helper-address

Use the `show ip helper-address` command to display the IP helper address configuration.

Syntax

`show ip helper-address [interface]`

- *interface* — Optionally specify an interface to limit the output to the configuration of a single interface. The interface is identified as `vlan vlan-id`.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Field Descriptions:

Interface	The relay configuration is applied to packets that arrive on this interface. This field is set to “any” for global IP helper entries.
UDP Port	The relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as “any” are applied to packets with the destination UDP ports listed in Table 4.
Discard	If “Yes”, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	The number of times the IP helper entry has been used to relay or discard a packet.
Server Address	The IPv4 address of the server to which packets are relayed.

Example

`show ip helper-address`

IP helper is enabled

Interface	UDP Port	Discard	Hit Count	Server Address
-----	-----	-----	-----	-----

vlan 100		dhcp	No	10
10.100.1.254				
10.100.2.254				
vlan 101		any	Yes	2
any		dhcp	No	0
10.200.1.254				

show ip helper statistics

Use the `show ip helper statistics` command to display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent.

Syntax

show ip helper statistics

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Field descriptions:

DHCP client messages received	The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL > 1 and having valid source and destination IP addresses.
DHCP client messages relayed	The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.
DHCP server messages received	The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
DHCP server messages relayed	The number of DHCP server messages relayed to a client.
UDP client messages received	The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
UDP client messages relayed	The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.
DHCP message hop count exceeded max	The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show bootpdhcrelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.

DHCP message with secs field below min	The number of DHCP client messages received with secs fields that are less than the minimum value. The minimum secs value is a configurable value and is displayed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with giaddr set to local address	The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurrence.
Packets with expired TTL	The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard relay entry.

Example

```
console#show ip helper statistics
```

```
DHCP client messages received..... 8
DHCP client messages relayed..... 2
DHCP server messages received..... 2
DHCP server messages relayed..... 2
UDP client messages received..... 8
UDP client messages relayed..... 2
DHCP message hop count exceeded max..... 0
DHCP message with secs field below min..... 0
DHCP message with giaddr set to local address.. 0
Packets with expired TTL..... 0
Packets that matched a discard entry..... 0
```


IP Routing Commands

This chapter explains the following commands:

- encapsulation
- ip address
- ip mtu
- ip netdirbroadcast
- ip route
- ip route default
- ip route distance
- ip routing
- routing
- show ip brief
- show ip interface
- show ip protocols
- show ip route
- show ip route preferences
- show ip route summary
- show ip stats
- vlan routing

encapsulation

Use the **encapsulation** command in Interface Configuration mode to configure the link layer encapsulation type for the packet. Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

Syntax

encapsulation {**ethernet** | **snap**}

- **ethernet** — Specifies Ethernet encapsulation.
- **snap** — Specifies SNAP encapsulation.

Default Configuration

Ethernet encapsulation is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example applies SNAP encapsulation for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#encapsulation snap
```

ip address

Use the **ip address** command in Interface Configuration mode to configure an IP address on an interface. Also use this command to configure one or more secondary IP addresses on the interface. This command changes the label IP address in the show IP interface.

Syntax

ip address *ip-address* {*subnet-mask* | *prefix-length*} [**secondary**]

no ip address *ip-address* { *subnet-mask* | *prefix-length* } [**secondary**]

- *ip-address* — IP address of the interface.
- *subnet-mask* — Subnet mask of the interface
- *prefix-length* — Length of the prefix. Must be preceded by a forward slash (/). (Range: 1-30 bits)
- **secondary** — Indicates the IP address is a secondary address.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Loopback) mode

User Guidelines

This command also implicitly enables the interface for routing (i.e. as if the user had issued the ‘routing’ interface command).

Example

The following example defines the IP address and subnet mask for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip address 192.168.10.10
255.255.255.0
```

ip mtu

Use the **ip mtu** command in Interface Configuration mode to set the IP Maximum Transmission Unit (MTU) on a routing interface. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Use the **no** form of the command to return the MTU size to the default value.

Software currently does not fragment IP packets. Packets forwarded in hardware ignore the IP MTU. Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface. Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP

stack uses its default IP MTU and ignores the value set using the **ip mtu** command. OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency (unless OSPF has been instructed to ignore differences in IP MTU with the **ip ospf mtuignore** command).

Syntax

ip mtu *integer*

- *integer*— Specifies the distance (preference) of an individual static route. (Range: 68-9198)

Default Configuration

1500 bytes is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example defines 1480 as the MTU for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip mtu 1480
```

ip netdirbcast

Use the **ip netdirbcast** command in Interface Configuration mode to enable the forwarding of network-directed broadcasts. When enabled, network directed broadcasts are forwarded. When disabled they are dropped. Use the no form of the command to disable the broadcasts.

Syntax

ip netdirbcast

`no ip netdirbcst`

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example defines the IP address and subnet mask for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip netdirbcst
```

ip route

Use the **ip route** command in Global Configuration mode to configure a static route. Use the **no** form of the command to delete the static route. The IP route command sets a value for the route preference. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. Specifying the preference of a static route controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

Syntax

ip route *ip addr* { *subnetmask* | *prefix length* } *nextHopRtr* [*preference*]

no ip route *ip addr* { *subnetmask* | *prefix length* } *nextHopRtr* [*preference*]

- *ip-address* — IP address of destination interface.
- *subnet-mask* — Subnet mask of destination interface.

- *prefix-length* — Length of prefix. Must be preceded with a forward slash (/). (Range: 0-32 bits)
- *nextHopRtr* — IP address of the next hop router.
- *preference* — Specifies the preference value, a.k.a. administrative distance, of an individual static route. (Range: 1-255)

Default Configuration

Default value of preference is 1.

Command Mode

Global Configuration mode

User Guidelines

For the static routes to be visible, you must:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Example

The following example identifies the *ip-address subnet-mask*, *next-hop-ip* and a preference value of 200.

```
console(config)#ip route 192.168.10.10 255.255.255.0
192.168.20.1 metric 200
```

ip route default

Use the **ip route default** command in Global Configuration mode to configure the default route. Use the no form of the command to delete the default route.

Syntax

ip route default *next-hop-ip* [*preference*]

no ip route default *next-hop-ip* [*preference*]

- *next-hop-ip* — IP address of the next hop router.

- *preference* — Specifies the preference value, a.k.a administrative distance, of an individual static route. (Range: 1-255)

Default Configuration

Default value of preference is 1.

Command Mode

Global Configuration mode

User Guidelines

For routed management traffic:

- 1 Router entries are checked for applicable destinations.
- 2 The globally assigned default-gateway is consulted.

Router entries take precedence over an assigned default-gateway.

Example

The following example identifies the *next-hop-ip* and a preference value of 200.

```
console(config)#ip route 192.168.10.10 255.255.255.0  
192.168.20.1 200
```

ip route distance

Use the **ip route distance** command in Global Configuration mode to set the default distance (preference) for static routes. Lower route preference values are preferred when determining the best route. The **ip route** and **ip route default** commands allow optional setting of the distance of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance are applied to static routes created after invoking the **ip route distance** command.

Syntax

ip route distance *integer*

no ip route distance *integer*

- *integer* — Specifies the distance (preference) of an individual static route. (Range 1-255)

Default Configuration

Default value of distance is 1.

Command Mode

Global Configuration mode

User Guidelines

Lower route distance values are preferred when determining the best route.

Example

The following example sets the default route metric to 80.

```
console(config)#ip route distance 80
```

ip routing

To globally enable IPv4 routing on the router, use the "ip routing" command in Global Configuration mode. To disable IPv4 routing globally, use the **no** form of this command.

Syntax

ip routing

no ip routing

Default Configuration

The ip routing default configuration is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use this command to globally enable IPv4 routing.

Example

```
console(config)#ip routing
```

routing

Use the **routing** command in Interface Configuration mode to enable IPv4 and IPv6 routing for an interface. View the current value for this function with the **show ip brief** command. The value is labeled Routing Mode in the output display. Use the no form of the command to disable routing for an interface.

Syntax

routing

no routing

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IPv4 and IPv6 routing for VLAN 15

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#routing
```

show ip brief

Use the **show ip brief** command in Privileged EXEC mode to display all the summary information of the IP.

Syntax

show ip brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IP summary information.

```
console#show ip brief
Default Time to Live..... 30
Routing Mode.....
Disabled
IP Forwarding Mode.....
Enabled
Maximum Next Hops..... 2
```

show ip interface

Use the **show ip interface** command in Privileged EXEC mode to display all pertinent information about one or more IP interfaces.

Syntax

show ip interface [vlan vlan-id | loopback loopback -id]

- *vlan-id*— Valid VLAN ID
- *loopback-id*— Valid loopback ID. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples display all IP information and information specific to VLAN 15.

```
console#show ip interface
```

Management Interface:

```
IP Address..... 10.240.4.125
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.240.4.1
Burned In MAC Address..... 00:10:18:82:04:35
Network Configuration Protocol Current..... None
Management VLAN ID..... 1
```

Routing Interfaces:

Netdir Multi

Interface	IP Address	IP Mask	Bcast	CastFwd
-----	-----	-----	-----	-----
vlan1	192.168.10.10	255.255.255.0	Disable	Disable
vlan2	0.0.0.0	0.0.0.0	Enable	Disable
loopback2	0.0.0.0	0.0.0.0	Disable	Disable

```
console#show ip interface vlan 15
Primary IP Address..... 192.168.10.10/255.255.255.0
Secondary IP Address(es)..... 192.168.20.20/255.255.255.0
Routing Mode..... Disable
Administrative Mode..... Disable
Forward Net Directed Broadcasts..... Disable
Proxy ARP..... Enable
Local Proxy ARP..... Disable
Active State..... Inactive
Link Speed Data Rate..... Inactive
MAC Address..... 00:00:00:01:00:02
Encapsulation Type..... Ethernet
IP MTU..... 1500
```

show ip protocols

Use the `show ip protocols` command in Privileged EXEC mode to display the parameters and current state of the active routing protocols.

Syntax

`show ip protocols`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays parameters and current state of active routing protocols.

```
console#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds
Invalid after 180 seconds, hold down 120, flushed
after 300
Redistributing: RIP, Static, OSPF
Default version control: send version 1, receive
version 1
Interfaces:
Interface Send Receive Key-chain
-----
176.1.1.1 1 1 flowers
176.2.1.1 passive 2
Routing Information Sources:
Gateway Last Update
176.1.1.2 0:00:17
Preference: 60
Routing Protocol is "ospf"
Redistributing: OSPF, External direct, Static, RIP
Interfaces:
Interface Metric Key-chain
-----
176.1.1.1 10 flowers
176.2.1.1 1
```

Routing Information Sources:

Gateway State

176.1.1.2 Full

External Preference: 60

Internal Preference: 20

show ip route

Use the **show ip route** command in Privileged EXEC mode to display the routing table.

Syntax

show ip route [*protocol* | *address ip-address* [*subnet-mask* | *prefix-length*]
[*longer-prefixes*]]

- *protocol*— Specifies the protocol that installed the routes. (Range: **connected**, **ospf**, **rip static**)
- *ip-address* — Specifies the network for which the route is to be displayed and displays the best matching best-route for the address.
- *subnet-mask* — Subnet mask of the IP address.
- *prefix-length* — Length of prefix, in bits. Must be preceded with a forward slash (/). (Range: 0-32 bits)
- **longer-prefixes** — Indicates that the *ip-address* and *subnet-mask* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the routing table.

```
console#show ip route
```

Route Codes: R - RIP Derived, O - OSPF Derived, C -
Connected, S - Static

B - BGP Derived, IA - OSPF Inter Area

E1 - OSPF External Type 1, E2 - OSPF External Type 2

N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA external type
2

show ip route preferences

Use the **show ip route preferences** command in Privileged EXEC mode displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values.

Syntax

```
show ip route preferences
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IP route preferences.

```
console#show ip route preferences
```

Local.....	0
Static.....	1
OSPF Intra-area routes.....	110
OSPF Inter-area routes.....	110
OSPF External routes.....	110
RIP.....	120

show ip route summary

Use the **show ip route summary** command in Privileged EXEC mode to display the routing table summary.

Syntax

show ip route summary [**all**]

- **all** — Shows the number of all routes, including best and non-best routes. To include only the number of best routes, do not use this optional parameter.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the IP route summary.

```
console#show ip route summary
```

```
Connected Routes..... 0
Static Routes..... 0
```


RIP Routes.....	0
OSPF Routes.....	0
Intra Area Routes.....	0
Inter Area Routes.....	0
External Type-1 Routes.....	0
External Type-2 Routes.....	0
Total routes.....	0

show ip stats

Use the **show ip stats** command in User EXEC mode to display IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Syntax

show ip stats

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IP route preferences.

```
console>show ip stats
IpInReceives..... 24002
IpInHdrErrors..... 1
IpInAddrErrors..... 925
```

IpForwDatagrams.....	0
IpInUnknownProtos.....	0
IpInDiscards.....	0
IpInDelivers.....	18467
IpOutRequests.....	295
IpOutDiscards.....	0
IpOutNoRoutes.....	0
IpReasmTimeout.....	0
IpReasmReqds.....	0
IpReasmOKs.....	0
IpReasmFails.....	0
IpFragOKs.....	0
IpFragFails.....	0
IpFragCreates.....	0
IpRoutingDiscards.....	0
IcmpInMsgs.....	3
IcmpInErrors.....	0
IcmpInDestUnreachs.....	0
IcmpInTimeExcds.....	0
IcmpInParmProbs.....	0
IcmpInSrcQuenchs.....	0
IcmpInRedirects.....	0
IcmpInEchos.....	3
IcmpInEchoReps.....	0
IcmpInTimestamps.....	0
IcmpInTimestampReps.....	0

IcmpInAddrMasks.....	0
IcmpInAddrMaskReps.....	0
IcmpOutMsgs.....	3
IcmpOutErrors.....	0
IcmpOutDestUnreachs.....	0
IcmpOutTimeExcds.....	0
IcmpOutParmProbs.....	0
IcmpOutSrcQuenchs.....	0
IcmpOutRedirects.....	0
IcmpOutEchoReps.....	3
IcmpOutTimestamps.....	0
IcmpOutTimestampReps.....	0
IcmpOutAddrMasks.....	0

vlan routing

Use this command to enable routing on a VLAN. Use the “no” form of this command to disable routing on a VLAN.

Syntax

vlan routing *vlanid* [*index*]

no vlan routing *vlanid*

vlanid — Valid VLAN ID (Range 1 – 4093).

index — Internal interface ID. This parameter is for NSF use only.

Default Configuration

Routing is not enabled on any VLANs by default.

Command Mode

VLAN Database mode

User Guidelines

The user is not required to use this command. Routing can still be enabled using the routing command in VLAN Interface Configuration mode.

Example

```
console(config-vlan)# vlan routing 10 1
```

IPv6 MLD Snooping Commands

This chapter explains the following commands:

- `ipv6 mld snooping immediate-leave`
- `ipv6 mld snooping groupmembership-interval`
- `ipv6 mld snooping maxresponse`
- `ipv6 mld snooping mcrtextpiretime`
- `ipv6 mld snooping (Global)`
- `ipv6 mld snooping (Interface)`
- `ipv6 mld snooping (VLAN)`
- `show ipv6 mld snooping`
- `show ipv6 mld snooping groups`

ipv6 mld snooping immediate-leave

The `ipv6 mld snooping immediate-leave` command enables or disables MLD Snooping `snooping immediate-leave` admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an MLD done message for that multicast group without first sending out MAC-based general queries to the interface. You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with MLD version 1 hosts.

Syntax

`ipv6 mld snooping immediate-leave [vlan-id]`

`no ipv6 mld snooping immediate-leave [vlan-id]`

- `vlan_id` — Specifies a VLAN ID value in VLAN Database mode.

Default Configuration

MLD Snooping fast-leave mode is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) Mode.

VLAN Database Mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-vlan)#ipv6 mld snooping immediate-leave 4
```

ipv6 mld snooping groupmembership-interval

The `ipv6 mld snooping groupmembership-interval` command sets the MLD Group Membership Interval time on a VLAN or interface. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the MLDv2 Maximum Response time value. The range is 2 to 3600 seconds.

Syntax

`ipv6 mld snooping groupmembership-interval [vlan-id] [seconds]`

`no ipv6 mld snooping groupmembership-interval [vlan-id]`

- `vlan_id` — Specifies a VLAN ID value in VLAN Database mode.
- `seconds` — MLD group membership interval time in seconds. (Range: 2-3600)

Default Configuration

The default group membership interval time is 260 seconds.

Command Mode

Interface Configuration mode.

VLAN Database mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-4/g1)#ipv6 mld snooping  
groupmembership-interval 300
```

ipv6 mld snooping maxresponse

The `ipv6 mld snooping maxresponse` command sets the MLD Maximum Response time for an interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an

interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD Query Interval time value. The range is 1 to 3599 seconds.

Syntax

ipv6 mld snooping maxresponse [*vlan-id*] [*seconds*]

no ipv6 mld snooping maxresponse [*vlan-id*]

- **vlan_id** — Specifies a VLAN ID value in VLAN Database mode.
- **seconds** — MLD maximum response time in seconds. (Range: 1–3599)

Default Configuration

The default maximum response time is 10 seconds.

Command Mode

Interface Configuration mode.

VLAN Database mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-4/g1)#ipv6 mld snooping maxresponse
33
```

ipv6 mld snooping mcrtexpiretime

The **ipv6 mld snooping mcrtexpiretime** command sets the Multicast Router Present Expiration time. The time is set for a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 1 to 3600 seconds.

Syntax

ipv6 mld snooping mcrtexpiretime [*vlan-id*] [*seconds*]

no ipv6 mld snooping mcertexpiretime [*vlan-id*]

- *vlan_id*— Specifies a VLAN ID value in VLAN Database mode.
- *seconds*— multicast router present expiration time in seconds. (Range: 1–3600)

Default Configuration

The default multicast router present expiration time is 300 seconds.

Command Mode

Interface Configuration mode.

VLAN Database mode.

User Guidelines

This command has no user guidelines

Example

```
console(config-if-4/g1)#ipv6 mld snooping  
mcertexpiretime 60
```

ipv6 mld snooping (Global)

The **ipv6 mld snooping (Global)** command enables MLD Snooping on the system (Global Config Mode).

Syntax

ipv6 mld snooping

no ipv6 mld snooping

Default Configuration

MLD Snooping is disabled.

Command Mode

Global Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 mld snooping
```

ipv6 mld snooping (Interface)

The **ipv6 mld snooping (Interface)** command enables MLD Snooping on an interface. If an interface has MLD Snooping enabled and it becomes a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if the interface is removed from a port-channel (LAG).

Syntax

```
ipv6 mld snooping
```

```
no ipv6 mld snooping
```

Default Configuration

MLD Snooping is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-4/g1)#ipv6 mld snooping
```

ipv6 mld snooping (VLAN)

The **ipv6 mld snooping (VLAN)** command enables MLD Snooping on a particular VLAN and enables MLD snooping on all interfaces participating in a VLAN.

Syntax

`ipv6 mld snooping vlan-id`

`no ipv6 mld snooping vlan-id`

- *vlan-id* — Specifies a VLAN ID value.

Default Configuration

MLD Snooping is disabled.

Command Mode

VLAN Database mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-vlan)#ipv6 mld snooping 1
```

show ipv6 mld snooping

The `show ipv6 mld snooping` command displays MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

Syntax

`show ipv6 mld snooping [interface {ethernet interface | port-channel port-channel-number} | vlan vlan-id]`

Default Configuration

This command has no default configuration

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

With no optional arguments, the command displays the following information:

- Admin Mode — Indicates whether or not MLD Snooping is active on the switch.
- Interfaces Enabled for MLD Snooping — Interfaces on which MLD Snooping is enabled.
- MLD Control Frame Count — This displays the number of MLD control frames that are processed by the CPU.
- VLANs Enabled for MLD Snooping — VLANs on which MLD Snooping is enabled.

When you specify an interface or VLAN, the following information displays:

- MLD Snooping Admin Mode — Indicates whether MLD Snooping is active on the interface or VLAN.
- Fast Leave Mode — Indicates whether MLD Snooping Fast-leave is active on the VLAN.
- Group Membership Interval — Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
- Max Response Time — Displays the amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
- Multicast Router Present Expiration Time — Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

show ipv6 mld snooping groups

The `show ipv6 mld snooping groups` command displays the MLD Snooping entries in the MFDB table.

Syntax

`show ipv6 mld snooping groups [{vlan vlan-id | address ipv6-multicast-address}]`

- *vlan_id* — Specifies a VLAN ID value.
- *ipv6-multicast-address* — Specifies an IPv6 Multicast address.

Default configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

To see the full Multicast address table (including static addresses) use the `show bridge address-table` command.

Example

```
console#show ipv6 mld snooping groups
```

Vlan	Ipv6 Address	Type	Ports
----	-----	-----	-----
1	3333.0000.0003	Dynamic	1/g1,1/g3
2	3333.0000.0004	Dynamic	1/g1,1/g3
2	3333.0000.0005	Dynamic	1/g1,1/g3

MLD Reporters that are forbidden statically:

```
-----
```

Vlan	Ipv6 Address	Ports
----	-----	-----

```
console#show ipv6 mld snooping groups vlan 2
```

Vlan	Ipv6 Address	Type	Ports
----	-----	-----	-----

2	3333.0000.0004	Dynamic	1/g1,1/g3
2	3333.0000.0005	Dynamic	1/g1,1/g3

```
MLD Reporters that are forbidden statically:
```

```
-----
```

Vlan	Ipv6 Address	Ports
----	-----	-----

IPv6 Multicast Commands

This chapter explains the following commands:

- `ipv6 pimsm` (Global config)
- `ipv6 pimsm` (VLAN Interface config)
- `ipv6 pimsm bsr-border`
- `ipv6 pimsm bsr-candidate`
- `ipv6 pimsm dr-priority`
- `ipv6 pimsm hello-interval`
- `ipv6 pimsm join-prune-interval`
- `ipv6 pimsm register-threshold`
- `ipv6 pimsm rp-address`
- `ipv6 pimsm rp-candidate`
- `ipv6 pimsm spt-threshold`
- `ipv6 pimsm ssm`
- `show ipv6 pimsm`
- `show ipv6 pimsm bsr`
- `show ipv6 pimsm interface`
- `show ipv6 pimsm neighbor`
- `show ipv6 pimsm rphash`
- `show ipv6 pimsm rp mapping`

ipv6 pimsm (Global config)

Use the **ipv6 pimsm** command to administratively enable of PIMSM for IPv6 multicast routing. Use the "no" form of this command to disable PIMSM for IPv6.

Syntax

```
ipv6 pimsm  
no ipv6 pimsm
```

Default Configuration

IPv6 PIMSM is disabled on the router by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pimsm
```

ipv6 pimsm (VLAN Interface config)

Use the **ipv6 pimsm** command in VLAN Interface configuration mode to administratively enable PIM-SM multicast routing mode on a particular IPv6 router interface. Use the "no" form of this command to disable PIM SM on an interface.

Syntax

```
ipv6 pimsm  
no ipv6 pimsm
```

Default Configuration

PIM-SM is disabled by default.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 pimsm
```

ipv6 pimsm bsr-border

Use the `ipv6 pimsm bsr-border` command to prevent bootstrap router (BSR) messages from being sent or received through an interface. Use the "no" form of this command to disable the interface from being the BSR border.

Syntax

```
ipv6 pimsm bsr-border
```

```
no ipv6 pimsm bsr-border
```

Default Configuration

BSR-border is disabled by default.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 pimsm bsr-border
```

ipv6 pimsm bsr-candidate

Use the **ipv6 pimsm bsr-candidate** command to configure the router to announce its candidacy as a bootstrap router (BSR). Use the "no" form of this command to stop the router from announcing its candidacy as a bootstrap router.

Syntax

ipv6 pimsm bsr-candidate *vlan* *vlan-id* *hash-mask-len* [*priority*]

no ipv6 pimsm bsr-candidate *vlan* *vlan-id*

- *vlan-id*—A valid VLAN ID value.
- *hash-mask-len*—The length of a mask that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups. (Range 0–128 bits).
- *priority*—The priority of the candidate BSR. The BSR with the higher priority is preferred. If the priority values are the same, the router with the higher IP address is the BSR. (Range: 0–255).

Default Configuration

The router will not announce its candidacy by default.

The default hash mask length is 126 bits.

The default priority is 0.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pimsm bsr-candidate vlan 9 10 34
```

ipv6 pimsm dr-priority

Use the **ipv6 pimsm dr-priority** command to set the priority value for which a router is elected as the designated router (DR). Use the "no" form of this command to set the priority to the default.

Syntax

ipv6 pimsm dr-priority *priority*

no ipv6 pimsm dr-priority

- *priority*—The election priority (Range: 0–2147483647).

Default Configuration

The default election priority is 1.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 pimsm dr-priority 10
```

ipv6 pimsm hello-interval

Use the **ipv6 pimsm hello-interval** command to configure the PIM-SM Hello Interval for the specified interface. Use the "no" form of this command to set the hello interval to the default.

Syntax

ipv6 pimsm hello-interval interval

no ipv6 pimsm hello-interval

- *interval*—The hello interval (Range: 0–65535 seconds).

Default Configuration

The default hello interval is 30 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 pimsm hello-interval 45
```

ipv6 pimsm join-prune-interval

Use the **ipv6 pimsm join-prune-interval** command to configure the interface join/prune interval for the PIM-SM router. Use the "no" form of this command to set the join/prune interval to the default.

Syntax

ipv6 pimsm join-prune-interval interval

no ipv6 pimsm join-prune-interval

- **interval**—The join/prune interval (Range: 0–18000 seconds).

Default Configuration

The default join/prune interval is 60 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 pimsm join-prune-  
interval 90
```

ipv6 pimsm register-threshold

Use the **ipv6 pimsm register-threshold** command to configure the Register Threshold rate for the RP router to switch to the shortest path. Use the "no" form of this command to set the register threshold rate to the default.

Syntax

ipv6 pimsm register-threshold *threshold*

no ipv6 pimsm register-threshold

- **threshold**—The threshold rate (Range: 0–2000 Kbps).

Default Configuration

The default threshold rate is 0.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pimsm register-threshold 250
```

ipv6 pimsm rp-address

Use the **ipv6 pimsm rp-address** command to statically configure the RP address for one or more multicast groups. The optional keyword **override** indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR. Use the "no" form of this command to remove the RP address for one or more multicast groups.

Syntax

ipv6 pimsm rp-address *rp-address group-address/prefixlength* [override]

no ipv6 pimsm rp-address

- *rp-address*—An RP address.
- *group-address*—The group address to display.
- *prefixlength*—This parameter specifies the prefix length of the IP address for the media gateway. (Range: 1–32)

Default Configuration

There are no static RP addresses configured by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pimsm rp-address 2001::1  
ff1e::/64
```

ipv6 pimsm rp-candidate

Use the **ipv6 pimsm rp-candidate** command to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR). Use the "no" form of this command to disable the router from advertising itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Syntax

ipv6 pimsm rp-candidate vlan *vlan-id group-address/prefixlength*

no ipv6 pimsm rp-candidate vlan *vlan-id*

- *vlan-id*—A valid VLAN ID value.
- *group-address*—The group address to display.

- **prefixlength**—This parameter specifies the prefix length of the IP address for the media gateway. (Range: 1–32)

Default Configuration

The router does not advertise itself as a PIM candidate rendezvous point by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pimsm rp-candidate vlan 6  
ff1e::/64
```

ipv6 pimsm spt-threshold

Use the **ipv6 pimsm spt-threshold** command to configure the Data Threshold rate for the last-hop router to switch to the shortest path. Use the "no" form of this command to set the data threshold to the default.

Syntax

ipv6 pimsm spt-threshold *threshold*

no ipv6 pimsm spt-threshold

- *threshold*—The threshold rate (Range: 0–2000 Kbps).

Default Configuration

The default threshold rate is 0.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pimsm spt-threshold 1000
```

ipv6 pimsm ssm

Use the **ipv6 pimsm ssm** command to define the Source Specific Multicast (SSM) range of multicast addresses.

Syntax

ipv6 pimsm ssm {default | group-address/prefixlength}

- **default**—Defines the SSM range access list to 232/8.
- **group-address**—Group IP address supported by RP.
- **prefixlength**—This parameter specifies the prefix length of the IP address for the media gateway. (Range: 1–32)

Default Configuration

There is no SSM range defined by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 pimsm ssm ff1e::/64
```

show ipv6 pimsm

Use the **show ipv6 pimsm** command to display global status of IPv6 PIMSM and its IPv6 routing interfaces.

Syntax

show ipv6 pimsm

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

console#show ipv6 pimsm

```
Admin Mode.....
Enabled

Data Threshold Rate (Kbps)..... 1000
Register Threshold Rate (Kbps)..... 250
```

```

                SSM RANGE TABLE
                Group Address/Prefix Length
                -----

FF1E::/64

        PIM-SM INTERFACE STATUS
Interface  Interface-Mode  Operational-Status
-----
vlan 3      Enabled          Operational
```

vlan 6	Enabled	Operational
vlan 9	Enabled	Operational

show ipv6 pimsm bsr

Use the **show ipv6 pimsm bsr** command to display the bootstrap router (BSR) information. The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

Syntax

```
show ipv6 pimsm bsr
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pimsm bsr
```

```
BSR Address.....
3001::1

BSR Priority..... 23

BSR Hash Mask Length..... 10

Next bootstrap message(hh:mm:ss) .....
00:00:11

Next Candidate RP advertisement(hh:mm:ss) .....
00:00:12
```

show ipv6 pimsm interface

Use the **show ipv6 pimsm interface** command to display interface configuration parameters. If no interface is specified, all interfaces are displayed.

Syntax

show ipv6 pimsm interface [*vlan *vlan-id**]

- *vlan-id*—A valid VLAN ID value.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pimsm interface vlan 6
```

```
Slot/Port..... vlan
6

IP Address.....
FE80::2FF:EDFF:FED0:2/128

Hello Interval (secs)..... 30

Join Prune Interval (secs)..... 60

Neighbor Count..... 0

Designated Router.....
FE80::2FF:EDFF:FED0:2

DR Priority..... 1
```

BSR Border.....
Disabled

show ipv6 pimsm neighbor

Use the `show ipv6 pimsm neighbor` command to display IPv6 PIMSM neighbors learned on the routing interfaces.

Syntax

`show ipv6 pimsm neighbor [all | interface vlan vlan-id]`

- *vlan-id* —A valid VLAN ID value.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pimsm neighbor all
Slot/Port..... vlan
6
Neighbor Address.....
FE80::200:FF:FE00:33
Up Time (hh:mm:ss).....
00:00:12
Expiry Time (hh:mm:ss).....
00:01:34
DR Priority..... 0
```

show ipv6 pimsm rphash

Use the `show ipv6 pimsm rphash` command to display which rendezvous point (RP) is being selected for a specified group.

Syntax

`show ipv6 pimsm rphash group-address`

group-address—Group IP address supported by RP.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pimsm rphash ff1e::/64
```

RP	Type
Address	
-----	----
3001::1	BSR

show ipv6 pimsm rp mapping

Use the `show ipv6 pimsm rp mapping` command to display all group-to-RP mappings of which the router is aware (either configured or learned from the bootstrap router (BSR)). If no RP is specified, all active RPs are displayed

Syntax

show ipv6 pimsm rp mapping [*rp-address*]

- *rp-address*—IP address of RP.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pimsm rp mapping
```

```
Group Address.....
FF1E::/64

RP Address.....
2001::1

origin.....
Static

Group Address.....
FF1E::/64

RP Address.....
3001::1

origin..... BSR
```

IPv6 Routing Commands

This chapter explains the following commands:

- clear ipv6 neighbors
- clear ipv6 statistics
- ipv6 address
- ipv6 enable
- ipv6 forwarding
- ipv6 host
- ipv6 mld last-member-query-count
- ipv6 mld last-member-query-interval
- ipv6 mld-proxy
- ipv6 mld-proxy reset-status
- ipv6 mld-proxy unsolicit-rprt-interval
- ipv6 mld query-interval
- ipv6 mld query-max-response-time
- ipv6 mld router
- ipv6 mtu
- ipv6 nd dad attempts
- ipv6 nd managed-config-flag
- ipv6 nd ns-interval
- ipv6 nd other-config-flag
- ipv6 nd prefix
- ipv6 nd ra-interval
- ipv6 nd ra-lifetime
- ipv6 nd reachable-time
- ipv6 nd suppress-ra
- ipv6 pimdm

- `ipv6 route`
- `ipv6 route distance`
- `ipv6 unicast-routing`
- `ping ipv6`
- `ping ipv6 interface`
- `show ipv6 brief`
- `show ipv6 interface`
- `show ipv6 mld groups`
- `show ipv6 mld interface`
- `show ipv6 mld-proxy`
- `show ipv6 mld-proxy groups`
- `show ipv6 mld-proxy groups detail`
- `show ipv6 mld-proxy interface`
- `show ipv6 mld traffic`
- `show ipv6 neighbors`
- `show ipv6 pimdm`
- `show ipv6 pimdm interface`
- `show ipv6 pimdm neighbor`
- `show ipv6 route`
- `show ipv6 route preferences`
- `show ipv6 route summary`
- `show ipv6 traffic`
- `show ipv6 vlan`
- `traceroute ipv6`

clear ipv6 neighbors

Use the **clear ipv6 neighbors** command in Privileged EXEC mode to clear all entries in the IPv6 neighbor table or an entry on a specific interface.

Syntax

clear ipv6 neighbors [*vlan *vlan-id**]

- *vlan-id*— Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example clears all entries in the IPv6 neighbor table.

```
console(config)#clear ipv6 neighbors
```

clear ipv6 statistics

Use the **clear ipv6 statistics** command in Privileged EXEC mode to clear IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces. IPv6 statistics display in the output of the **show ipv6 traffic** command.

Syntax

clear ipv6 statistics [*vlan *vlan-id**] **tunnel** *tunnel-id* | **loopback** *loopback-id*]

- *vlan-id*— Valid VLAN ID.
- *tunnel-id*— Tunnel identifier. (Range: 0-7)
- *loopback-id*— Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example clears IPv6 statistics for VLAN 11.

```
console(config)#clear ipv6 statistics vlan 11
```

ipv6 address

Use the **ipv6 address** command in Interface Configuration mode to configure an IPv6 address on an interface (including tunnel and loopback interfaces) and to enable IPv6 processing on this interface. Multiple globally reachable addresses can be assigned to an interface by using this command. There is no need to assign a link-local address by using this command since one is automatically created. IPv6 addresses can be expressed in eight blocks. Also of note is that instead of a period, a colon separates each block. For simplification, leading zeros of each 16-bit block can be omitted. One sequence of 16-bit blocks containing only zeros can be replaced with a double colon “::”, but not more than one at a time (otherwise it is no longer a unique representation).

Dropping zeros: 3ffe:ffff:100:f101:0:0:0:1 becomes 3ffe:ffff:100:f101::1

Local host: 0000:0000:0000:0000:0000:0000:0000:0001 becomes ::1

Any host: 0000:0000:0000:0000:0000:0000:0000:0000 becomes ::

The hexadecimal letters in the IPv6 addresses are not case-sensitive. An example of an IPv6 prefix and prefix length is 3ffe:1::1234/64.

Syntax

ipv6 address *prefix/prefix-length* [**eui64**]

no ipv6 address [*prefix/prefix-length*] [**eui64**]

- *prefix* — Consists of the bits of the address to be configured.
- *prefix-length* — Designates how many of the high-order contiguous bits of the address make up the prefix.
- *eui64* — The optional eui-64 field designates that IPv6 processing on the interfaces is enabled using an EUI-64 interface ID in the low order 64 bits of the address. If this option is used, the value of *prefix-length* must be 64 bits.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures an IPv6 address and enables IPv6 processing.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 address 2020:1::1/64
```

ipv6 enable

Use the **ipv6 enable** command in Interface Configuration mode to enable IPv6 routing on an interface (including tunnel and loopback interfaces) that has not been configured with an explicit IPv6 address. Command execution automatically configures the interface with a link-local address. The command is not required if an IPv6 global address is configured on the interface.

Syntax

ipv6 enable

no ipv6 enable

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example enables IPv6 routing, which has not been configured with an explicit IPv6 address.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 enable
```

ipv6 forwarding

Use the **ipv6 forwarding** command in Global Configuration mode to enable IPv6 forwarding on a router.

Syntax

```
ipv6 forwarding
no ipv6 forwarding
```

Default Configuration

Enabled is the default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example globally enables IPv6 forwarding.

```
console#configure
console(config)#ipv6 forwarding
console(config)#no ipv6 forwarding
```

ipv6 host

The **ipv6 host** command is used to define static host name-to- ipv6 address mapping in the host cache.

Syntax

ipv6 host *name ipv6-address*

no ipv6 host *name*

- *name* — Host name.
- *ipv6-address* — IPv6 address of the host.

Default Configuration

No IPv6 hosts are defined.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config)#ipv6 host Dell 2001:DB8::/32
```

ipv6 mld last-member-query-count

The `ipv6 mld last-member-query-count` command sets the number of listener-specific queries sent before the router assumes that there are no local members on the interface. Use the “no” form of this command to set the last member query count to the default.

Syntax

`ipv6 mld last-member-query-count last-member-query-count`

`no ipv6 mld last-member-query-count`

- *last-member-query-count* — Query count (Range: 1–20).

Default Configuration

The default last member query count is 2.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 mld last-member-query-count 5
```

ipv6 mld last-member-query-interval

The `ipv6 mld last-member-query-interval` command sets the last member query interval for the MLD interface, which is the value of the maximum response time parameter in the group-specific queries sent out of this interface. Use the “no” form of this command to set the last member query interval to the default.

Syntax

`ipv6 mld last-member-query-interval last-member-query-interval`

no ipv6 mld last-member-query-interval

- *last-member-query-interval*— The last member query interval (Range: 0–65535 milliseconds).

Default Configuration

The default last member query interval is 1 second.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 mld last-member-query-  
interval 5000
```

ipv6 mld-proxy

Use the **ipv6 mld-proxy** command to enable MLD Proxy on the router. To enable MLD Proxy on the router, you must also enable multicast forwarding. Also, ensure that there are no other multicast routing protocols enabled on the router. Use the “no” form of this command to disable MLD Proxy.

Syntax

ipv6 mld-proxy

no ipv6 mld-proxy

Default Configuration

MLD Proxy is disabled by default.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 mld-proxy
```

ipv6 mld-proxy reset-status

Use the **ipv6 mld-proxy reset-status** command to reset the host interface status parameters of the MLD Proxy router. This command is only valid when MLD Proxy is enabled on the interface.

Syntax

```
ipv6 mld-proxy reset-status
```

Command Mode

Interface Configuration (VLAN) mode.

Default Configuration

There is no default configuration for this command.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 mld-proxy reset-status
```

ipv6 mld-proxy unsolicit-rprt-interval

Use the **ipv6 mld-proxy unsolicit-rprt-interval** command to set the unsolicited report interval for the MLD Proxy router. This command is only valid when MLD Proxy is enabled on the interface. Use the “no” form of this command to reset the MLD Proxy router's unsolicited report interval to the default value.

Syntax

`ipv6 mld-proxy unsolicited-report-interval interval`

`no ipv6 mld-proxy unsolicited-report-interval`

- *interval*—The interval between unsolicited reports (Range: 1–260 seconds).

Default Configuration

The unsolicited report interval is 1 second by default.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines

Example

```
console(config-if-vlan3)#ipv6 mld-proxy unsolicit-  
rprt-interval 10
```

ipv6 mld query-interval

The `ipv6 mld query-interval` command sets the MLD router's query interval for the interface. The query-interval is the amount of time between the general queries sent when the router is querying on that interface. Use the “no” form of this command to set the query interval to the default.

Syntax

`ipv6 mld query-interval query-interval`

`no ipv6 mld query-interval`

- *query-interval*—Query interval (Range: 1–3600).

Default Configuration

The default query interval is 125 seconds.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 mld query-interval 130
```

ipv6 mld query-max-response-time

The `ipv6 mld query-max-response-time` command sets MLD query maximum response time for the interface. This value is used in assigning the maximum response time in the query messages that are sent on that interface. Use the “no” form of this command to set the maximum query response time to the default.

Syntax

```
ipv6 mld query-max-response-time query-max-response-time
```

```
no ipv6 mld query-max-response-time
```

- *query-max-response-time* — Maximum query response time (Range: 1–65535 milliseconds).

Default Configuration

The default query maximum response time is 10 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 mld query-max-response-time 4500
```

ipv6 mld router

The **ipv6 mld router** command is used to enable MLD in the router in global configuration mode and for a specific interface in interface configuration mode. Use the “no” form of this command to disable MLD.

Syntax

ipv6 mld router

no ipv6 mld router

Default Configuration

MLD is disabled by default.

Command Mode

Global Configuration mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 mld router
```

ipv6 mtu

Use the **ipv6 mtu** command in Interface Configuration mode to set the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface.

When the **ipv6 mtu** is at its default value (1500) and has not been configured, a subsequent decrease change to the link mtu results in a reduction of the **ipv6 mtu**.

Syntax

ipv6 mtu *mtu*

no ipv6 mtu

- *mtu* — Is the maximum transmission unit. (Range: 1280-1500)

Default Configuration

The default MTU is 1500.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 mtu 1300
```

ipv6 nd dad attempts

Use the **ipv6 nd dad attempts** command in Interface Configuration mode to set the number of duplicate address detection probes transmitted while doing neighbor discovery. Duplicate address detection verifies that an IPv6 address on an interface is unique.

Syntax

ipv6 nd dad attempts *attempts*

no ipv6 nd dad attempts

- *attempts* — Probes transmitted. (Range: 0-600)

Default Configuration

The default value for attempts is 1.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets at 10 the number of duplicate address detection probes transmitted while doing neighbor discovery.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd dad attempts 10
```

ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command in Interface Configuration mode to set the “managed address configuration” flag in router advertisements. When the value is true,

end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.

Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

Default Configuration

False is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

In the following example, the end node uses DHCPv6.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd managed-config-flag
```

ipv6 nd ns-interval

Use the **ipv6 nd ns-interval** command in Interface Configuration mode to set the interval between router advertisements for advertised neighbor solicitations. An advertised value of 0 means the interval is unspecified.

Syntax

```
ipv6 nd ns-interval milliseconds
```

```
no ipv6 nd ns-interval
```

- *milliseconds* — Interval duration. (Range: 0, 1000–4294967295)

Default Configuration

0 is the default value for *milliseconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the interval between router advertisements for advertised neighbor solicitations at 5000 ms.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd ns-interval 5000
```

ipv6 nd other-config-flag

Use the `ipv6 nd other-config-flag` command in Interface Configuration mode to set the “other stateful configuration” flag in router advertisements sent from the interface.

Syntax

`ipv6 nd other-config-flag`

`no ipv6 nd other-config-flag`

Default Configuration

False is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets to true the “other stateful configuration” flag in router advertisements

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ipv6 nd other-config-flag
```

ipv6 nd prefix

Use the **ipv6 nd prefix** command to configure parameters associated with prefixes that the router advertises in its router advertisements.

Syntax

ipv6 nd prefix *prefix/prefix-length* [{ *valid-lifetime* | infinite} { *preferred-lifetime* | infinite}] [**no-autoconfig**] [**off-link**]

no ipv6 nd prefix *prefix/prefix-length*

- *prefix* — IPv6 prefix.
- *prefix-length* — IPv6 prefix length.
- *valid-lifetime* — Valid lifetime of the router in seconds. (Range: 0–4294967295 seconds)
- infinite — Indicates lifetime value is infinite.
- *preferred-lifetime* — Preferred-lifetime of the router in seconds. (Range: 0–4294967295 seconds)
- **no-autocoding** — Do not use Prefix for autoconfiguration.
- **off-link** — Do not use Prefix for onlink determination.

Default Configuration

604800 seconds is the default value for valid-lifetime, 2592000 seconds for preferred lifetime.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

The router advertises its global IPv6 prefixes in its router advertisements (RAs). An RA only includes the prefixes of the IPv6 addresses configured on the interface where the RA is transmitted. Addresses are configured using the **ipv6 address** interface configuration command. Each prefix advertisement includes information about the prefix, such as its lifetime values and whether hosts should use the prefix for on-link determination or address auto-configuration. Use the **ipv6 nd prefix** command to configure these values.

The `ipv6 nd prefix` command will allow you to preconfigure RA prefix values before you configure the associated interface address. In order for the prefix to be included in RAs, you must configure an address that matches the prefix using the `ipv6 address` command. Prefixes specified using `ipv6 nd prefix` without an associated interface address will not be included in RAs and will not be committed to the device configuration.

Example

The following example sets the IPv6 prefixes to include in the router advertisement.

```
console(config)#interface vlan 11
console(config-if-vlan11)#ipv6 nd prefix 2020:1::1/64
```

ipv6 nd ra-interval

Use the `ipv6 nd ra-interval` command in Interface Configuration mode to set the transmission interval between router advertisements.

Syntax

`ipv6 nd ra-interval maximum minimum`

`no ipv6 nd ra-interval`

- *maximum* — The maximum interval duration (Range: 4–1800 seconds).
- *minimum* — The minimum interval duration (Range: 3 – (0.75 * maximum) seconds).

Default Configuration

600 is the default value for *seconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

The minimum interval cannot be larger than 75% of the maximum interval.

Example

The following example sets the transmission interval between router advertisements at 1000 seconds.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd ra-interval 1000
```

ipv6 nd ra-lifetime

Use the **ipv6 nd ra-lifetime** command in Interface Configuration mode to set the value that is placed in the Router Lifetime field of the router advertisements sent from the interface.

Syntax

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

- *seconds* — Lifetime duration. The value must be zero, or it must be an integer between the value of the router advertisement transmission interval and 9000 seconds. A value of zero means this router is not to be used as the default router. (Range: 0-9000)

Default Configuration

1800 is the default value for *seconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets at 1000 seconds the value that is placed in the Router Lifetime field of the router advertisements.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 nd ra-lifetime 1000
```

ipv6 nd reachable-time

Use the **ipv6 nd reachable-time** command in Interface Configuration mode to set the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation.

Syntax

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

- *milliseconds* — Reachable-time duration. A value of zero means the time is unspecified by the router. (Range: 0-3600000 milliseconds)

Default Configuration

The default value for neighbor discovery reachable times is 0 milliseconds.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the router advertisement time at 5000 milliseconds to consider a neighbor reachable after neighbor discovery confirmation.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ipv6 nd reachable-time 5000
```

ipv6 nd suppress-ra

Use the **ipv6 nd suppress-ra** command in Interface Configuration mode to suppress router advertisement transmission on an interface.

Syntax

```
ipv6 nd suppress-ra  
no ipv6 nd suppress-ra
```

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example suppresses router advertisement transmission.

```
console(config)#interface vlan 15  
console(config-if-vlan15)#ipv6 nd suppress-ra
```

ipv6 pimdm

Use the **ipv6 pimdm** command to enable PIM-DM Multicast Routing Mode across the router in global configuration mode or on a specific routing interface in interface mode. Use the “no” form of this command to disable PIM-DM.

Syntax

```
ipv6 pimdm  
no ipv6 pimdm
```

Default Configuration

IPv6 PIM-DM is disabled by default.

Command Mode

Global Configuration mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ipv6 pimdm
```

ipv6 pimdm hello-interval

The `ipv6 pimdm hello-interval` command is used to configure the PIM-DM Hello Interval for the specified router interface. The Hello-interval is to be specified in seconds. Use the "no" form of this command to reset the hello interval to the default.

Syntax

`ipv6 pimdm hello-interval interval`

`no ipv6 pimdm hello-interval`

- `interval` - The hello interval time in seconds (Range: 0–65535).

Default Configuration

The default hello interval is 30 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan5)#ipv6 pimdm hello-interval  
500
```

ipv6 route

Use the **ipv6 route** command in Global Configuration mode to configure an IPv6 static route.

Syntax

ipv6 route *ipv6-prefix/prefix-length* [Null | **interface** {**tunnel** *tunnel-id* | **vlan** *vlan-id*}] *next-hop-address* [*preference*]

no ipv6 route *ipv6-prefix/prefix-length* [Null | **interface** {**tunnel** *tunnel-id* | **vlan** *vlan-id*}] *next-hop-address*

- *ipv6-prefix* — Is the IPv6 network that is the destination of the static route.
- *prefix-length* — Is the length of the IPv6 prefix — a decimal value (usually 0-64) that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede it.
- **interface** — Identifies direct static routes from point-to-point and broadcast interfaces, and must be specified when using a link-local address as the next hop.
- **tunnel or vlan** — Is the tunnel or vlan interface to associate with the route.
- *next-hop-address* — Is the IPv6 address of the next hop that can be used to reach the specified network.
- *preference* — Is a value the router uses to compare this route with routes from other route sources that have the same destination. (Range: 1-255)

Default Configuration

1 is the default value for *preference*.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configure an IPv6 static route.

```
console(config)#ipv6 route 2020:1::1/64 2030:1::2
```

ipv6 route distance

Use the **ipv6 route distance** command in Global Configuration mode to set the default distance (preference) for static routes. Lower route preference values are preferred when determining the best route. The **ipv6 route** and **ipv6 route default** commands allow optional setting of the distance of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance is applied to static routes created after invoking the **ipv6 route distance** command.

Syntax

ipv6 route distance *integer*

no ipv6 route distance *integer*

- *integer* — Specifies the distance (preference) of an individual static route. (Range 1-255)

Default Configuration

Default value of *integer* is 1.

Command Mode

Global Configuration mode

User Guidelines

Lower route distance values are preferred when determining the best route.

Example

The following example sets the default distance to 80.

```
console(config)#ipv6 route distance 80
```

ipv6 unicast-routing

Use the **ipv6 unicast-routing** command in Global Configuration mode to enable forwarding of IPv6 unicast datagrams.

Syntax

ipv6 unicast-routing

no ipv6 unicast-routing

Default Configuration

Disabled is the default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example globally enables Ipv6 unicast datagram forwarding.

```
console(config)#ipv6 unicast-routing
```

```
console(config)#no ipv6 unicast-routing
```

ping ipv6

Use ping ipv6 command in Privileged EXEC mode to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected

through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

Syntax

`ping ipv6 {ip-address | hostname} [size size]`

- *ipv6-address* — Target IPv6 address to ping.
- *hostname* — Hostname to ping (contact). (Range: 1–158 characters)
- *size* — Size of the datagram. (Range: 48–2048 bytes)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example determines whether another computer is on the network at the IPv6 address specified.

```
console(config)#ping ipv6 2030:1::1/64
```

```
Send count=3, Receive count=0 from 2030:1::1/64
```

```
Average round trip time = 0.00 ms
```

ping ipv6 interface

Use `ping ipv6 interface` command in the Privileged EXEC mode to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there

is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the **interface** keyword to ping an interface by using the link-local address or the global IPv6 address of the interface. The source can be a loopback, tunnel, or logical interface.

Syntax

ping ipv6 interface {**vlan** *vlan-id*| **tunnel** *tunnel-id*} | **loopback** *loopback-id*} *link-local-address* [**size** *datagram-size*]

- *vlan-id* — Valid VLAN ID.
- *tunnel-id* — Tunnel identifier. (Range: 0-7)
- *loopback-id* — Loopback identifier. (Range: 0-7)
- *link-local-address* — IPv6 address to ping.
- *datagram-size* — Size of the datagram. (Range: 48-2048 bytes)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example determines whether another computer is on the network at the IPv6 address specified.

```
console(config)#ping ipv6 interface loopback 1  
FE80::202:BCFF:FE00:3068/128
```

```
Send count=3, Receive count=0 from  
FE80::202:BCFF:FE00:3068/128
```

```
Average round trip time = 0.00 ms
```

show ipv6 brief

Use the **show ipv6 brief** command in Privileged EXEC mode to display the IPv6 status of forwarding mode and IPv6 unicast routing mode.

Syntax

show ipv6 brief

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the IPv6 status of forwarding mode and IPv6 unicast routing mode.

```
console#show ipv6 brief
```

```
IPv6 Forwarding Mode..... Enable
```

```
IPv6 Unicast Routing Mode..... Disable
```

```
IPv6 Hop Limit.....1
```

show ipv6 interface

Use the **show ipv6 interface** command in Privileged EXEC mode to show the usability status of IPv6 interfaces.

Syntax

show ipv6 interface {**brief** | **loopback** *loopback-id* | **tunnel** *tunnel-id* | **vlan** *vlan-id* [**prefix**]}

- *loopback-id* — Valid loopback interface ID

- *tunnel-id*— Valid tunnel interface ID
- *vlan-id*— Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples show the usability status of a IPv6 VLAN interface individually and all IPv6 interfaces collectively in an abbreviated format.

```
console#show ipv6 interface vlan 3

IPv6 is enabled

IPv6 Prefix is.....
FE80::2FC:E3FF:FE90:147/128
                                     3FF0:1236:C261::1/64

Routing Mode..... Enabled
Administrative Mode..... Enabled
IPv6 Routing Operational Mode..... Enabled
Interface Maximum Transmit Unit..... 1500
Router Duplicate Address Detection Transmits... 1
Router Advertisement NS Interval..... 0
Router Lifetime Interval..... 1800
Router Advertisement Reachable Time..... 0
Router Advertisement Interval..... 600
Router Advertisement Managed Config Flag..... Disabled
Router Advertisement Other Config Flag..... Disabled
```

```
Router Advertisement Suppress Flag..... Disabled
```

```
Prefix 3FF0:1236:C261::1/64
```

```
Preferred Lifetime..... 10000
```

```
Valid Lifetime..... 100000
```

```
Onlink Flag..... Enabled
```

```
Autonomous Flag..... Enabled
```

```
console#show ipv6 interface brief
```

Interface	Oper.	Mode	IPv6 Address/Length

vlan3	Enabled		FE80::2FC:E3FF:FE90:147/128 3FF0:1236:C261::1/64
loopback 1	Enabled		FE80::2FC:E3FF:FE90:145/128 3FF0:C221:1234::1/64
loopback 2	Disabled		
tunnel 1	Disabled		3FFE:1234::1/64 [TENT]

show ipv6 mld groups

The **show ipv6 mld groups** command is used to display information about multicast groups that MLD reported. The information is displayed only when MLD is enabled on at least one interface. If MLD was not enabled on any interfaces, there is no group information to be displayed.

Syntax

show ipv6 mld groups {*group-address* | **vlan** *vlan-id*}

- *group-address* — The group address to display.
- *vlan-id* — A valid VLAN id.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The following fields are displayed as a table when **vlan *vlan-id*** is specified:

Number of (*, G) entries	Displays the number of groups present in the MLD Table.
Number of (S, G) entries	Displays the number of include and exclude mode sources present in the MLD Table.
Group Address	The address of the multicast group.
Interface	Interface through which the multicast group is reachable.
Uptime	Time elapsed in seconds since the multicast group has been known.
Expiry Time	Time left in seconds before the entry is removed from the MLD membership table.

If **vlan *vlan-id*** is not specified, the following fields are displayed for each multicast group and each interface:

Group Address	The address of the multicast group.
Interface	Interface through which the multicast group is reachable.
Uptime	Time elapsed in seconds since the multicast group has been known.
Expiry Time	Time left in seconds before the entry is removed from the MLD membership table of this interface.
Last Reporter	The IP Address of the source of the last membership report received for this multicast group address on that interface.
Filter Mode	The filter mode of the multicast group on this interface. The values it can take are INCLUDE and EXCLUDE.

Compatibility Mode	The compatibility mode of the multicast group on this interface. The values it can take are MLDv1 and MLDv2.
Version 1 Host Timer	The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.

The following table is displayed to indicate all the sources associated with this group:

Source Address	The IP address of the source.
Uptime	Time elapsed in seconds since the source has been known.
Expiry Time	Time left in seconds before the entry is removed.

Example

```
console#show ipv6 mld groups ff1e::5
```

```
Interface..... vlan 6
Group Address..... FF1E::5
Last Reporter.....
FE80::200:FF:FE00:22
Up Time (hh:mm:ss)..... 00:03:43
Expiry Time (hh:mm:ss)..... -----
Filter Mode..... Include
Version1 Host Timer..... -----
Group compat mode..... v2
Source Address      ExpiryTime
-----
4001::6             00:03:15
4001::7             00:03:15
4001::8             00:03:15
```

```
console#show ipv6 mld groups vlan 6
```

```

Group Address..... FF1E::1
Interface..... vlan 6
Up Time (hh:mm:ss)..... 00:04:23
Expiry Time (hh:mm:ss)..... -----

```

```

Group Address..... FF1E::2
Interface..... vlan 6
Up Time (hh:mm:ss)..... 00:04:23
Expiry Time (hh:mm:ss)..... -----

```

```

Group Address..... FF1E::3
Interface..... vlan 6
Up Time (hh:mm:ss)..... 00:04:23
Expiry Time (hh:mm:ss)..... -----

```

```

Group Address..... FF1E::4
Interface..... vlan 6
Up Time (hh:mm:ss)..... 00:04:23
Expiry Time (hh:mm:ss)..... -----

```

show ipv6 mld interface

The `show ipv6 mld interface` command is used to display MLD related information for an interface.

Syntax

```
show ipv6 mld interface {vlan vlan-id | all}
```

- *vlan-id*— A valid VLAN id.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The following information is displayed for the specified interface:

Interface	The interface number in unit/slot/port format.
MLD Global Admin Mode	This field displays the configured global administrative status of MLD.
MLD Interface Admin Mode	This field displays the configured interface administrative status of MLD.
MLD Operational Mode	The operational status of MLD on the interface.
MLD Version	This field indicates the version of MLD configured on the interface.
Query Interval	This field indicates the configured query interval for the interface.
Query Max Response Time	This field indicates the configured maximum query response time (in seconds) advertised in MLD queries on this interface.
Robustness	This field displays the configured value for the tuning for the expected packet loss on a subnet attached to the interface.
Startup Query Interval	This value indicates the configured interval between General Queries sent by a Querier on startup.
Startup Query Count	This value indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	This value indicates the configured Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.

The following information is displayed if the operational mode of the MLD interface is enabled:

Querier Status	This value indicates whether the interface is a MLD querier or non-querier on the subnet with which it is associated.
Querier Address	The IP address of the MLD querier on the subnet the interface with which it is associated.
Querier Up Time	Time elapsed in seconds since the querier state has been updated.
Querier Expiry Time	Time left in seconds before the Querier losses its title as querier.
Wrong Version Queries	Indicates the number of queries received whose MLD version does not match the MLD version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Leaves	The number of times a group membership has been removed on this interface.
Number of Groups	The current number of membership entries for this interface.

Example

```
console#show ipv6 mld interface vlan 2
```

```
Interface..... vlan 2
MLD Global Admin Mode..... Enabled
MLD Interface Admin Mode..... Disabled
MLD Operational Mode..... Disabled
MLD Version..... 2
Query Interval (secs)..... 100
Query Max Response Time(milli-secs)..... 1111
Robustness..... 2
Startup Query Interval (secs)..... 31
Startup Query Count..... 2
```

```
Last Member Query Interval (milli-secs)..... 1111
Last Member Query Count..... 2
```

show ipv6 mld-proxy

Use the **show ipv6 mld-proxy** command to display a summary of the host interface status parameters.

Syntax

show ipv6 mld-proxy

Command Mode

Privileged EXEC mode

Default Configuration

There is no default configuration for this command.

User Guidelines

The command displays the following parameters only when you enable MLD Proxy:

Interface Index	The interface number of the MLD Proxy interface.
Admin Mode	Indicates whether MLD Proxy is enabled or disabled. This is a configured value.
Operational Mode	Indicates whether MLD Proxy is operationally enabled or disabled. This is a status parameter.
Version	The present MLD host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the MLD-Proxy interface.
Unsolicited Report Interval	The time interval at which the MLD-Proxy interface sends unsolicited group membership reports.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (MLD-Proxy interface).

Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Proxy Start Frequency	The number of times the MLD-Proxy has been stopped and started.

Example

```
console#show ipv6 mld-proxy
Interface Index..... vlan 10
Admin Mode..... Enabled
Operational Mode..... Enabled
Version..... 3
Num of Multicast Groups..... 0
Unsolicited Report Interval..... 1
Querier IP Address on Proxy Interface..... fe80::1:2:5
Older Version 1 Querier Timeout..... 00:00:00
Proxy Start Frequency.....1
```

show ipv6 mld-proxy groups

Use the `show ipv6 mld-proxy groups` command to display information about multicast groups that the MLD Proxy reported.

Syntax

```
show ipv6 mld-proxy groups
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

The following parameters are displayed by this command:

Interface	The MLD Proxy interface.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group on the network attached to the MLD-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: <ul style="list-style-type: none"> • Idle_Member—The interface has responded to the latest group membership query for this group. • Delay_Member—The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.

Example

```
console#show ipv6 mld-proxy groups
```

```
Interface..... vlan 10
```

```
Group Address Last Reporter Up Time Member State Filter Mode
Sources
```

```
-----
FF1E::1 FE80::100:2.3 00:01:40 DELAY_MEMBER Exclude 2
FF1E::2 FE80::100:2.3 00:02:40 DELAY_MEMBER Include 1
FF1E::3 FE80::100:2.3 00:01:40 DELAY_MEMBER Exclude 0
FF1E::4 FE80::100:2.3 00:02:44 DELAY_MEMBER Include 4
```

show ipv6 mld-proxy groups detail

Use the **show ipv6 mld-proxy groups detail** command to display information about multicast groups that MLD Proxy reported.

Syntax

```
show ipv6 mld-proxy groups detail
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

The following parameters are displayed by this command:

Interface	The interface number of the MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group on the network attached to the MLD Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: <ul style="list-style-type: none">• Idle_Member—The interface has responded to the latest group membership query for this group.• Delay_Member—The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	The time left for a source to get deleted.

Example

```
console#show ipv6 igmp-proxy groups
Interface.....  vlan 10

Group Address Last Reporter    Up Time    Member State    Filter
Mode    Sources
```


FF1E::1 FE80::100:2.3 244 DELAY_MEMBER Exclude
2

Group Source List	Expiry Time
-----	-----

2001::1	00:02:40
---------	----------

2001::2	-----
---------	-------

FF1E::2 FE80::100:2.3 243 DELAY_MEMBER Include
1

Group Source List	Expiry Time
-----	-----

3001::1	00:03:32
---------	----------

3002::2	00:03:32
---------	----------

FF1E::3 FE80::100:2.3 328 DELAY_MEMBER Exclude
0

FF1E::4 FE80::100:2.3 255 DELAY_MEMBER Include
4

Group Source List	Expiry Time
-----	-----

4001::1	00:03:40
---------	----------

5002::2	00:03:40
---------	----------

4001::2	00:03:40
---------	----------

5002::2	00:03:40
---------	----------

show ipv6 mld-proxy interface

Use the `show ipv6 mld-proxy interface` command to display a detailed list of the host interface status parameters.

Syntax

`show ipv6 mld-proxy interface`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

The following parameters are displayed only when MLD Proxy is enabled:

Interface	The MLD Proxy interface.
-----------	--------------------------

The column headings of the table associated with the interface are as follows:

Ver	The MLD version.
Query Rcvd	Number of MLD queries received.
Report Rcvd	Number of MLD reports received.
Report Sent	Number of MLD reports sent.
Leaves Rcvd	Number of MLD leaves received. Valid for version 2 only.
Leaves Sent	Number of MLD leaves sent on the Proxy interface. Valid for version 2 only.

Example

```
console#show ipv6 mld-proxy interface
```

```
Interface..... vlan 10
```


Ver	Query	Rcvd	Report	Rcvd	Report	Sent	Leave	Rcvd	Leave	Sent

1	2		0		0		0		2	
2	3		0		4		-----		-----	

show ipv6 mld traffic

The `show ipv6 mld traffic` command is used to display MLD statistical information for the router.

Syntax

`show ipv6 mld traffic`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The following fields are displayed:

Valid MLD Packets Received	The number of valid MLD packets received by the router.
Valid MLD Packets Sent	The number of valid MLD packets sent by the router.
Queries Received	The number of valid MLD queries received by the router.
Queries Sent	The number of valid MLD queries sent by the router.
Reports Received	The number of valid MLD reports received by the router.
Reports Sent	The number of valid MLD reports sent by the router.
Leaves Received	The number of valid MLD leaves received by the router.
Leaves Sent	The number of valid MLD leaves sent by the router.

Bad Checksum MLD Packets	The number of bad checksum MLD packets received by the router.
Malformed MLD Packets	The number of malformed MLD packets received by the router.

Example

```
console#show ipv6 mld traffic
```

```
Valid MLD Packets Received..... 52
Valid MLD Packets Sent..... 7
Queries Received..... 0
Queries Sent..... 7
Reports Received..... 52
Reports Sent..... 0
Leaves Received..... 0
Leaves Sent..... 0
```

show ipv6 neighbors

Use the `show ipv6 neighbors` command in Privileged EXEC mode to display information about the IPv6 neighbors.

Syntax

```
show ipv6 neighbors
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the IPv6 neighbors.

```
console(config)#show ipv6 neighbors
```

```
Neighbor Last
```

IPv6 Address	MAC
Address	isRtr State Updated

```
Interface
```

```
-----
```

show ipv6 pimdm

The `show ipv6 pimdm` command is used to display PIM-DM Global Configuration parameters and PIM DM interface status.

Syntax

```
show ipv6 pimdm
```

Command Mode

Privileged EXEC mode.

Default Configuration

There is no default configuration for this command.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pimdm
```

```
Admin Mode.....
Enable
```

PIM-DM INTERFACE STATUS

Interface	Interface Mode	Protocol State
-----	-----	-----
vlan 10	Enable	Non-Operational
vlan 20	Enable	Non-Operational

show ipv6 pimdm interface

The `show ipv6 pimdm interface` command is used to display PIM-DM Configuration information for all interfaces or for the specified interface. If no interface is specified, Configuration of all interfaces is displayed.

Syntax

```
show ipv6 pimdm interface [vlan vlan-id | all]
```

- `vlan vlan-id` — A valid VLAN ID.
- `all` — To show configuration information for all valid interfaces.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pimdm interface vlan 10
```

```

Slot/Port..... vlan
10

IP Address.....
FE80::221:9BFF:FEC3:1216/128

Neighbor Count..... 0

Hello Interval (secs)..... 30

Designated Router..... Not
Supported

```

```
console#show ipv6 pimdm interface all
```

Address	Interface	Neighbor Count	Hello Interval
-----	-----	-----	-----
192.168.37.6	vlan 10	2	30
192.168.36.129	vlan 20	2	30
10.1.37.2	vlan 24	1	30

show ipv6 pimdm neighbor

The `show ipv6 pimdm neighbor` command is used to display PIM-DM Neighbor information including Neighbor Address, Uptime and Expiry time for all interfaces or for the specified interface.

Syntax

```
show ipv6 pimdm neighbor [interface vlan vlan-id | all]
```

- `vlan vlan-id`— A valid VLAN ID.
- `all` — To show neighbor information for all valid interfaces.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ipv6 pimdm neighbor interface vlan 10
```

		Up Time	Expiry Time
Neighbor Addr	Interface	hh:mm:ss	hh:mm:ss

show ipv6 route

Use the `show ipv6 route` command in Privileged EXEC mode to display the IPv6 routing table.

Syntax

```
show ipv6 route [{ipv6-address [protocol]} | {{ipv6-prefix/ipv6-prefix-length | interface} [protocol]} | protocol [all] | all}]
```

- *ipv6-address* — Specifies an IPv6 address for which the best-matching route would be displayed.
- *protocol* — Specifies the protocol that installed the routes. Is one of the following keywords: connected, ospf, static.
- *ipv6-prefix/ipv6 prefix-length* — Specifies a IPv6 network for which the matching route would be displayed.
- *interface* — Valid IPv6 interface. Specifies that the routes with next-hops on the selected interface be displayed.
- **all** — Specifies that all routes including best and non-best routes are displayed. Otherwise, only the best routes are displayed. If the connected keyword is selected for protocol, the **all** option is not available because there are no best or non-best connected routes.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the IPv6 routing table.

```
console(config)#show ipv6 route
```

```
IPv6 Routing Table - 0 entries
```

```
Codes: C - connected, S - static
```

```
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2  
- OSPF Ext 2
```

```
ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2
```

show ipv6 route preferences

Use the **show ipv6 route preferences** command in Privileged EXEC mode to show the preference value associated with the type of route. Lower numbers have a greater preference.

Syntax

```
show ipv6 route preferences
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows the preference value associated with the type of route.

```
console#show ipv6 route preferences
```

```
Local..... 0
Static..... 1
OSPF Intra-area routes..... 110
OSPF Inter-area routes..... 110
OSPF External routes..... 110
```

show ipv6 route summary

Use the **show ipv6 route summary** command in Privileged EXEC mode to display a summary of the routing table. Use **all** to display the count summary for all routes, including best and non-best routes. Use the command without parameters to display the count summary for only the best routes.

Syntax

```
show ipv6 route summary [all]
```

- **all** — Displays the count summary for all routes.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary of the routing table.

```
console#show ipv6 route summary

IPv6 Routing Table Summary - 0 entries

Connected Routes..... 0
Static Routes..... 0
OSPF Routes..... 0
Intra Area Routes..... 0
Inter Area Routes..... 0
External Type-1 Routes..... 0
External Type-2 Routes..... 0
Total routes..... 0
Number of Prefixes:
```

show ipv6 traffic

Use the **show ipv6 traffic** command in User EXEC mode to show traffic and statistics for IPv6 and ICMPv6.

Syntax

show ipv6 traffic [**vlan** *vlan-id* | **tunnel** *tunnel-id* | **loopback** *loopback-id*]

- *vlan-id* — Valid VLAN ID, shows information about traffic on a specific interface or, without the optional parameter, shows information about traffic on all interfaces.
- **tunnel** — Tunnel identifier. (Range: 0-7)
- **loopback** — Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following examples show traffic and statistics for IPv6 and ICMPv6, first for all interfaces and an individual VLAN.

```
console> show ipv6 traffic
IPv6 STATISTICS
Total Datagrams Received..... 0
Received Datagrams Locally Delivered..... 0
Received Datagrams Discarded Due To Header Errors..... 0
Received Datagrams Discarded Due To MTU..... 0
Received Datagrams Discarded Due To No Route..... 0
Received Datagrams With Unknown Protocol..... 0
Received Datagrams Discarded Due To Invalid Address..... 0
Received Datagrams Discarded Due To Truncated Data..... 0
Received Datagrams Discarded Other..... 0
Received Datagrams Reassembly Required..... 0
Datagrams Successfully Reassembled..... 0
Datagrams Failed To Reassemble..... 0
Datagrams Forwarded..... 0
Datagrams Locally Transmitted..... 0
Datagrams Transmit Failed..... 0
Datagrams Successfully Fragmented..... 0
Datagrams Failed To Fragment..... 0
Fragments Created..... 0
Multicast Datagrams Received..... 0
```

```
Multicast Datagrams Transmitted..... 0
```

```
console> show ipv6 traffic vlan 11
```

```
Interface..... 11
```

```
IPv6 STATISTICS
```

```
Total Datagrams Received..... 0
```

```
Received Datagrams Locally Delivered..... 0
```

```
Received Datagrams Discarded Due To Header Errors..... 0
```

```
Received Datagrams Discarded Due To MTU..... 0
```

```
Received Datagrams Discarded Due To No Route..... 0
```

```
Received Datagrams With Unknown Protocol..... 0
```

```
Received Datagrams Discarded Due To Invalid Address..... 0
```

```
Received Datagrams Discarded Due To Truncated Data..... 0
```

```
Received Datagrams Discarded Other..... 0
```

```
Received Datagrams Reassembly Required..... 0
```

```
Datagrams Successfully Reassembled..... 0
```

```
Datagrams Failed To Reassemble..... 0
```

```
Datagrams Forwarded..... 0
```

```
Datagrams Locally Transmitted..... 0
```

```
Datagrams Transmit Failed..... 0
```

```
Datagrams Successfully Fragmented..... 0
```

```
Datagrams Failed To Fragment..... 0
```

```
Fragments Created..... 0
```

```
Multicast Datagrams Received..... 0
```

```
Multicast Datagrams Transmitted..... 0
```

show ipv6 vlan

Use the `show ipv6 vlan` command in Privileged EXEC mode to display IPv6 VLAN routing interface addresses.

Syntax

```
show ipv6 vlan
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays IPv6 VLAN routing interface addresses.

```
console#show ipv6 vlan
```

```
MAC Address used by Routing VLANs: 00:02:BC:00:30:68
```

```
VLAN ID   IPv6 Address/Prefix Length
```

```
-----
```

```
1
```

traceroute ipv6

Use the **traceroute ipv6** command in Privileged EXEC mode to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.

Syntax

```
traceroute ipv6 {ip-address | hostname} [port]
```

- *ipv6-address* — Destination IPv6 address.
- *hostname* — Hostname to ping (contact). (Range: 1–158 characters)
- *port* — UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. (Range: 0–65535)

Default Configuration

33434 is the default port value.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example discovers the packet routes on a hop-by-hop basis.

```
console#traceroute ipv6 2020:1::1
```

Tracing route over a maximum of 20 hops

```
1 * N * N * N
```


Loopback Interface Commands

This chapter explains the following commands:

- interface loopback
- show interfaces loopback

interface loopback

Use the **interface loopback** command in Global Configuration mode to enter the Interface Loopback configuration mode.

Syntax

interface loopback *loopback-id*

no interface loopback *loopback-id*

- *loopback-id* — Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example enters the Interface Loopback 1 configuration mode.

```
console(config)# interface loopback 1
```

```
console(config-if-loopback1)#
```

show interfaces loopback

Use the **show interfaces loopback** command in Privileged EXEC mode to display information about one or all configured loopback interfaces.

Syntax

show interfaces loopback [*loopback-id*]

- *loopback-id* — Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Examples

The following examples display information about configured loopback interfaces.

```
console# show interfaces loopback

Loopback Id  Interface  IP Address  Received  Sent
              Packets  Packets
-----
1             loopback   1 0.0.0.0   0         0

console# show interfaces loopback 1

Interface Link Status..... Up
IP Address..... 0.0.0.0 0.0.0.0
MTU size..... 1500 bytes
```


Multicast Commands

This chapter explains the following commands:

- ip mcast boundary
- ip mroute
- ip multicast
- ip multicast ttl-threshold
- ip pimsm
- ip pimsm bsr-border
- ip pimsm bsr-candidate
- ip pimsm dr-priority
- ip pimsm hello-interval
- ip pimsm join-prune-interval
- ip pimsm register-threshold
- ip pimsm rp-address
- ip pimsm rp-candidate
- ip pimsm spt-threshold
- ip pimsm ssm
- show bridge multicast address-table count
- show ip mcast
- show ip mcast boundary
- show ip mcast interface
- show ip mcast mroute
- show ip mcast mroute group
- show ip mcast mroute source
- show ip mcast mroute static
- show ip pimsm bsr
- show ip pimsm interface

- show ip pimsm rphash
- show ip pimsm rp mapping

ip mcast boundary

Use the **ip mcast boundary** command in Interface Configuration mode to add an administrative scope multicast boundary specified by *groupipaddr* and *mask* for which this multicast administrative boundary is applicable. *groupipaddr* is a group IP address and *mask* is a group IP mask.

Syntax

ip mcast boundary *groupipaddr mask*

no ip mcast boundary *groupipaddr mask*

- *groupipaddr* — IP address of multicast group. Valid range is 239.0.0.0 to 239.255.255.255.
- *mask* — IP mask of multicast group.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example adds an administrative scope multicast boundary.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip mcast boundary 239.5.5.5  
255.255.255.255
```

ip mroute

Use the **ip mroute** command to create a static multicast route for a source range. Use the "no" form of this command to delete a static multicast route.

Syntax

ip mroute *source-address source-mask rpf-address preference*

no ip mroute *source-address source*

- *source-address* — The IP address of the multicast data source.
- *source-mask* — The IP subnet mask of the multicast data source.
- *rpf-address* — The IP address of the next hop towards the source.
- *preference* — The cost of the route (Range: 1 - 255).

Default Configuration

There is no default configuration for this command.

Command Mode

Global Configuration mode

Usage Guidelines

There are no user guidelines for this command.

Example

```
console(config)#
```

```
console(config)#ip mroute 1.1.1.1 255.255.0.0  
192.168.20.1 34
```

ip multicast

Use the **ip multicast** command in Global Configuration mode to set the administrative mode of the IP multicast forwarder in the router to active. For multicast routing to become operational, IGMP must be currently enabled. An error message is displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Syntax

ip multicast

no ip multicast

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables IP multicast on the router.

```
console#configure
console(config)#ip multicast
console(config)#no ip multicast
```

ip multicast ttl-threshold

Use the **ip multicast ttl-threshold** command in Interface Configuration mode to apply a *ttlvalue* to a routing interface. *ttlvalue* is the TTL threshold which is applied to the multicast Data packets forwarded through the interface.

Syntax

ip multicast ttl-threshold *ttlvalue*

no ip multicast ttl-threshold

- *ttlvalue* — Specifies TTL threshold. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example applies a *ttlvalue* of 5 to the VLAN 15 routing interface.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip multicast ttl-threshold
5
```

ip pimsm

The **ip pimsm** command is used to administratively enable PIM-SM multicast routing mode on a particular router interface. Use the “no” form of this command to disable PIM SM on an interface. This command deprecates the **ip pimsm mode** command.

Syntax

```
ip pimsm
no ip pimsm
```

Default Configuration

PIM-SM is disabled by default.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ip pimsm
```


ip pimsm bsr-border

The `ip pimsm bsr-border` command is used to prevent bootstrap router (BSR) messages from being sent or received through an interface. Use the “no” form of this command to disable the interface from being the BSR border.

Syntax

`ip pimsm bsr-border`

`no ip pimsm bsr-border`

Default Configuration

The interface is not enabled to send BSR messages by default.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ip pimsm bsr-border
```

ip pimsm bsr-candidate

The `ip pimsm bsr-candidate` command is used to configure the router to announce its candidacy as a bootstrap router (BSR). Use the “no” form of this command to stop the router from announcing its candidacy as a bootstrap router. This command deprecates the `ip pimsm cbsrhashmasklength` and `ip pimsm cbsrpreference` commands.

Syntax

`ip pimsm bsr-candidate vlan vlanid [hash-mask-length [priority]]`

`no ip pimsm bsr-candidate vlan vlanid`

- *vlanid*— A valid VLAN ID.

- *hash-mask-length* — The length of a mask that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups. (Range 0–32 bits).
- *priority* — The priority of the candidate BSR. The BSR with the higher priority is preferred. If the priority values are the same, the router with the higher IP address is the BSR. (Range 0–255).

Default Configuration

The router will not announce its candidacy by default

The default hash mask length is 32 bits.

The default priority is 0.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip pimsm bsr-candidate interface vlan
3 12 255
```

ip pimsm dr-priority

The **ip pimsm dr-priority** command is used to set the priority value for which a router is elected as the designated router (DR). Use the “no” form of this command to set the priority to the default.

Syntax

ip pimsm dr-priority *priority*

no ip pimsm dr-priority

- *priority* — The election priority (Range: 0–2147483647).

Default Configuration

The default election priority is 1.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ip pimsm dr-priority 12
```

ip pimsm hello-interval

The **ip pimsm hello-interval** command is used to configure the PIM-SM Hello Interval for the specified interface. Use the “no” form of this command to set the hello interval to the default. This command deprecates the **ip pimsm query-interval** command.

Syntax

ip pimsm hello-interval *interval*

no ip pimsm hello-interval

- *interval*— The hello interval (Range: 0–65535 seconds).

Default Configuration

The default hello interval is 30 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ip pimsm hello-interval 60
```

ip pimsm join-prune-interval

The **ip pimsm join-prune-interval** command is used to configure the interface join/prune interval for the PIM-SM router. Use the “no” form of this command to set the join/prune interval to the default. This command deprecates the **ip pimsm message-interval** command.

Syntax

```
ip pimsm join-prune-interval interval
```

```
no ip pimsm join-prune-interval
```

- *interval* — The join/prune interval (Range: 0–18000 seconds).

Default Configuration

The default join/prune interval is 60 seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan3)#ip pimsm join-prune-interval  
125
```

ip pimsm register-threshold

The **ip pimsm register-threshold** command is used to configure the Register Threshold rate for the RP router to switch to the shortest path. Use the “no” form of this command to set the register threshold rate to the default. This command deprecates the **ip pimsm register rate limit** command.

Syntax

ip pimsm register-threshold *threshold*

no ip pimsm register-threshold

- *threshold* — The threshold rate (Range: 0–2000 Kbps).

Default Configuration

The default threshold rate is 0. Previously, the default was 50.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip pimsm register-threshold 1000
```

ip pimsm rp-address

The **ip pimsm rp-address** command is used to statically configure the RP address for one or more multicast groups. The optional keyword **override** indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR. Use the “no” form of this command to remove the RP address for one or more multicast groups. This command deprecates the **ip pimsm staticrp** command.

Syntax

ip pimsm rp-address *rp-address group-address group-mask* [**override**]

no ip pimsm rp-address *rp-address group-address group-mask*

- *rp-address* — IP address of RP.
- *group-address* — Group IP address supported by RP.
- *group-mask* — Group subnet mask for group address.
- **override** — Override a conflicting address learned by BSR.

Default Configuration

There are no static RP addresses configured by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip pimsm rp-address 192.168.20.1 225.1.0.0  
255.255.255.0
```

ip pimsm rp-candidate

The **ip pimsm rp-candidate** command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR). Use the “no” form of this command to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR). This command deprecates the **ip pimsm crppreference** command.

Syntax

ip pimsm rp-candidate *vlan* *vlanid* *group-address* *group-mask*

ip pimsm rp-candidate *vlan* *vlanid*

- *vlanid* — A valid VLAN ID.
- *group-address* — Group IP address supported by RP.
- *group-mask* — Group subnet mask for group address.

Default Configuration

The router does not advertise itself as a PIM candidate rendezvous point by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip pimsm rp-candidate interface vlan
3 225.2.0.0 255.255.0.0
```

ip pimsm spt-threshold

The **ip pimsm spt-threshold** command is used to configure the Data Threshold rate for the last-hop router to switch to the shortest path. Use the “no” form of this command to set the data threshold to the default.

Syntax

ip pimsm spt-threshold *threshold*

no ip pimsm spt-threshold

- *threshold*— The threshold rate (Range: 0–2000 Kbps).

Default Configuration

The default data threshold is 0.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip pimsm spt-threshold 1000
```

ip pimsm ssm

The **ip pimsm ssm** command is used to define the Source Specific Multicast (SSM) range of IP multicast addresses. Use the “no” form of this command to disable the SSM range.

Syntax

`ip pimsm ssm {default | group-address group-mask}`

`no ip pimsm ssm`

- `default` — Defines the SSM range access list to 232/8.
- `group-address group-mask` — defines the SSM range.

Default Configuration

There is no SSM range defined by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip pimsm ssm default
```

```
console(config)#ip pimsm ssm 224.1.0.0 255.255.0.0
```

show bridge multicast address-table count

Use the `show bridge multicast address-table count` command to view statistical information about the entries in the multicast address table.

Syntax

`show bridge multicast address-table count`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following command shows information about the entries in the multicast address table.

```
console#show bridge multicast address-table count
```

Capacity: 1024

Used: 4

Static addresses: 2

Dynamic addresses: 1

Forbidden addresses: 1

The following table shows the information the command displays:

Field	Description
Capacity	The maximum number of addresses that can be stored in the multicast address table.
Used	The total number of addresses in the multicast address table.
Static addresses	The number of addresses in the multicast address table that are static IP addresses.
Dynamic addresses	The number of addresses in the multicast address table that were learned dynamically.
Forbidden addresses	The number of addresses in the multicast address table that are forbidden IP addresses.

show ip mcast

Use the **show ip mcast** command in Privileged EXEC mode to display the system-wide multicast information.

Syntax

`show ip mcast`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays system-wide multicast information.

```
console#show ip mcast
Admin Mode..... Enabled
Protocol State..... Non-Operational
Table Max Size..... 256
Protocol..... PIMDM
Multicast Forwarding Cache Entry Count..... 0
```

show ip mcast boundary

Use the `show ip mcast boundary` command in Privileged EXEC mode to display all the configured administrative scoped multicast boundaries.

Syntax

`show ip mcast boundary {vlan vlan-id | all}`

- *vlan-id*— Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all the configured administrative scoped multicast boundaries.

```
console#show ip mcast boundary all
```

```
MULTICAST BOUNDARY
```

```
Interface  Group  Ip Mask
```

```
-----
```

show ip mcast interface

Use the **show ip mcast interface** command in Privileged EXEC mode to display the multicast information for the specified interface.

Syntax

```
show ip mcast interface {vlan vlan-id | all}
```

- *vlan-id* — Valid Ethernet port

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the multicast information for VLAN 15.

```
console#show ip mcast interface vlan 15
Interface    TTL
-----
```

show ip mcast mroute

Use the `show ip mcast mroute` command in Privileged EXEC mode to display a summary or all the details of the multicast table.

Syntax

```
show ip mcast mroute {detail | summary}
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a summary or all the details of the multicast table.

```
console#show ip mcast mroute summary
Multicast Route Table Summary

Source IP      Group IP      Protocol      Incoming      Outgoing
-----      -
Interface      Interface List

console#show ip mcast mroute detail
Multicast Route Table
```

Source Ip	Group Ip	Expiry Time (secs)	Up Time (secs)	RPF Neighbor	Flags
-----	-----	-----	-----	-----	-----

show ip mcast mroute group

Use the **show ip mcast mroute group** command in Privileged EXEC mode to display the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the *groupipaddr* value.

Syntax

show ip mcast mroute group *groupipaddr* {detail | summary}

- groupipaddr* — IP address of the multicast group.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces.

```
console#show ip mcast mroute group 224.5.5.5 summary
```

Multicast Route Table Summary

Source IP	Group IP	Protocol	Incoming Interface	Outgoing Interface	List
-----	-----	-----	-----	-----	-----

```
console#show ip mcast mroute group 224.5.5.5 detail
Multicast Route Table

Source Ip Group Ip      Expiry      Up Time
Time(secs)   (secs)      RPF Neighbor  Flags
-----
```

show ip mcast mroute source

Use the **show ip mcast mroute source** command in Privileged EXEC mode to display the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the *sourceipaddr* or *sourceipaddr | groupipaddr* pair value(s).

Syntax

```
show ip mcast mroute source sourceipaddr {summary | groupipaddr}
```

- *sourceipaddr*— IP address of source.
- *groupipaddr*— IP address of multicast group.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays multicast configuration settings.

```
console#show ip mcast mroute source 10.1.1.1 summary
Multicast Route Table Summary

Source IP  Group IP      Protocol  Incoming  Outgoing
Interface Interface List
-----
```

```
console#show ip mcast mroute source 10.1.1.1 224.5.5.5
Multicast Route Table

Source IP      Group IP      Expiry      Up Time
Time(secs)    (secs)
-----
RPF Neighbor  Flags
```

show ip mcast mroute static

Use the `show ip mcast mroute static` command in Privileged EXEC mode to display all the static routes configured in the static mcast table if it is specified or display the static route associated with the particular *sourceipaddr*.

Syntax

`show ip mcast mroute static [sourceipaddr]`

- *sourceipaddr* — IP address of source.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the static routes configured in the static mcast table.

```
console#show ip mcast mroute static
```

MULTICAST STATIC ROUTES			
Source IP	Source Mask	RPF Address	Preference
1.1.1.1	255.255.255.0	2.2.2.2	23

show ip pimsm bsr

The **show ip pimsm bsr** command displays the bootstrap router (BSR) information. The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement. This command deprecates the **show ip pimsm componenttable** command.

Syntax

show ip pimsm bsr

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The following information is displayed:

BSR address	IP address of the BSR.
Uptime	Length of time that this router has been up (in hours, minutes, and seconds).
BSR Priority	Priority as configured in the ip pimsm bsr-candidate command.
Hash mask length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. This value is configured in the ip pimsm bsr-candidate command.
Next bootstrap message in	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP advertisement in	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.
RP	List of IP addresses of RPs.

Example

```
console#show ip pimsm bsr
```

```
BSR Address..... 1.1.1.1
BSR Priority..... 20
BSR Hash Mask Length..... 10
Next bootstrap message (hh:mm:ss) ..... 00:00:11
Next Candidate RP advertisement (hh:mm:ss) ..... 00:00:00
```

show ip pimsm interface

The **show ip pimsm interface** command displays interface config parameters. If no interface is specified, all interfaces are displayed. This command deprecates the **show ip pimsm interface stats** command.

Syntax

```
show ip pimsm interface [vlan vlan-id]
```

- *vlan-id* — A valid VLAN ID.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip pimsm interface vlan 3
```

```
Slot/Port..... vlan 3
IP Address..... 1.1.1.1
Subnet Mask..... 255.255.255.0
Hello Interval (secs)..... 30
Join Prune Interval (secs)..... 60
Neighbor Count..... 0
Designated Router..... 1.1.1.1
DR Priority..... 1
BSR Border..... Disabled
```

show ip pimsm rphash

The **show ip pimsm rphash** command displays which rendezvous point (RP) is being selected for a specified group.

Syntax

```
show ip pimsm rphash group-address
```

- *group-address* — Group IP address supported by RP.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The following fields are displayed:

RPAAddress of the RP for the group specified

OriginIndicate by which mechanism (BSR or static) the RP was selected.

Example

```
console#show ip pimsm rphash 225.1.0.5
```

RP Address	Type
-----	-----
1.1.1.1	Static

show ip pimsm rp mapping

The **show ip pimsm rp mapping** command is used to display all group-to-RP mappings of which the router is aware (either configured or learned from the bootstrap router (BSR)). If no RP is specified, all active RPs are displayed. This command deprecates the **show ip pimsm rp candidate**, **show ip pimsm staticrp** and **show ip pimsm rp** commands.

Syntax

```
show ip pimsm rp mapping [rp-address]
```

rp-address — An RP address.

Default configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip pimsm rp mapping
```

```
Group Address..... 225.1.0.0
Group Mask..... 255.255.255.0
RP Address..... 1.1.1.1
origin..... Static
Group Address..... 225.2.0.0
Group Mask..... 255.255.255.0
RP Address..... 2.2.2.2
origin..... BSR
```

OSPF Commands

This chapter explains the following commands:

- area default-cost
- area nssa
- area nssa default-info-originate
- area nssa no- redistribute
- area nssa no-summary
- area nssa translator-role
- area nssa translator-stab-intv
- area range
- area stub
- area stub no-summary
- area virtual-link
- area virtual-link authentication
- area virtual-link dead-interval
- area virtual-link hello-interval
- area virtual-link retransmit-interval
- area virtual-link transmit-delay
- auto-cost
- bandwidth
- capability opaque
- clear ip ospf
- default-information originate
- default-metric
- distance ospf
- distribute-list out
- enable

- exit-overflow-interval
- external-lsdb-limit
- ip ospf area
- ip ospf authentication
- ip ospf cost
- ip ospf dead-interval
- ip ospf hello-interval
- ip ospf mtu-ignore
- ip ospf network
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- maximum-paths
- passive-interface default
- nsf
- nsf helper
- nsf helper strict-lsa-checking
- nsf restart-interval
- passive-interface default
- passive-interface
- redistribute
- router-id
- router ospf
- show ip ospf
- show ip ospf abr
- show ip ospf area
- show ip ospf asbr
- show ip ospf database
- show ip ospf database database-summary

- show ip ospf interface
- show ip ospf interface brief
- show ip ospf interface stats
- show ip ospf neighbor
- show ip ospf range
- show ip ospf statistics
- show ip ospf stub table
- show ip ospf virtual-link
- show ip ospf virtual-link brief
- timers spf
- 1583compatibility

area default-cost

Use the **area default-cost** command in Router OSPF Configuration mode to configure the monetary default cost for the stub area. Use the **no** form of the command to return the cost to the default value.

Syntax

area *area-id* **default-cost** *integer*

no area *area-id* **default-cost**

- *area-id*— Identifies the OSPF stub area to configure. (Range: IP address or decimal from 0-4294967295)
- *integer*— The default cost for the stub area. (Range: 1-16777215)

Default Configuration

10 is the default configuration for *integer*.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example identifies a stub area of 10 and default cost of 100.

```
console(config)#router ospf
```

```
console(config-router)#area 10 default-cost 100
```

area nssa

Use the **area nssa** command in Router OSPF Configuration mode to configure the specified area ID to function as an NSSA. Use the **no** form of the command to disable NSSA from the specified area ID.

Syntax

area *area-id* nssa

no area *area-id* nssa

- *area-id* — Identifies the OSPF not-so-stubby-area. (Range: 0–4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures not-so-stubby-area 10 as an NSSA.

```
console(config)#router ospf
```

```
console(config-router)#area 10 nssa
```

area nssa default-info-originate

Use the **area nssa default-info-originate** command in Router OSPF Configuration mode to configure the metric value and type for the default route advertised into the NSSA. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2). Use the **no** form of the command to return the metric value and type to the default value.

Syntax

area *area-id* nssa default-info-originate [*integer*] [comparable | non-comparable]

no area *area-id* nssa default-info-originate

- *area-id* — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)

- *integer* — Specifies the metric of the default route advertised to the NSSA. (Range: 1–16777214)
- *comparable* — A metric type of nssa-external 1
- *non-comparable* — A metric type of nssa-external 2

Default Configuration

If no metric is defined, 10 is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the metric value and type for the default route advertised into the NSSA.

```
console(config-router)#area 20 nssa default-info-  
originate 250 non-comparable
```

area nssa no-redistribute

Use the **area nssa no-redistribute** command in Router OSPF Configuration mode to configure the NSSA Area Border router (ABR) so that learned external routes are not redistributed to the NSSA.

Syntax

area *area-id* **nssa no-redistribute**

no area *area-id* **nssa no-redistribute**

- *area-id* — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the NSSA ABR.

```
console(config-router)#area 20 nssa no-redistribute
```

area nssa no-summary

Use the **area nssa no-summary** command in Router OSPF Configuration mode to configure the NSSA so that summary LSAs are not advertised into the NSSA.

Syntax

area *area-id* **nssa no-summary**

no area *area-id* **nssa no-summary**

- *area-id* — Identifies the OSPF NSSA to configure. (Range: 0–4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the NSSA so that summary LSAs are not advertised into the NSSA.

```
console(config-router)#area 20 nssa no-summary
```

area nssa translator-role

Use the **area nssa translator-role** command in Router OSPF Configuration mode to configure the translator role of the NSSA.

Syntax

area *area-id* **nssa translator-role** {always | candidate}

no area *area-id* **nssa translator-role**

- *area-id* — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)
- always — The router assumes the role of the translator when it becomes a border router.
- candidate — The router to participate in the translator election process when it attains border router status.

Default Configuration

The default role is candidate.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the translator role of the NSSA.

```
console(config-router)#area 20 nssa translator-role  
always
```

area nssa translator-stab-intv

Use the **area nssa translator-stab-intv** command in Router OSPF Configuration mode to configure the translator stability interval of the NSSA.

Syntax

area *area-id* **nssa translator-stab-intv** *integer*

no area *area-id* **nssa translator-stab-intv**

- *area-id* — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)
- *integer* — The period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposited by another router. (Range: 0–3600)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the translator stability interval of the area 20 NSSA.

```
console(config-router)#area 20 nssa translator-stab-intv 2000
```

area range

Use the **area range** command in Router OSPF Configuration mode to configure a summary prefix for routes learned in a given area. There are two types of area ranges. An area range can be configured to summarize intra-area routes. An ABR advertises the range rather than the specific intra-area route as a type 3 summary LSA. Also, an area range can be configured at the edge of an NSSA to summarize external routes reachable within the NSSA. The range is advertised as a type 5 external LSA.

Syntax

area *area-id* **range** *ip-address subnet-mask* {**summarylink** | **nssaexternallink**}
[**advertise** | **not-advertise**]

no area *area-id* **range** *ip-address subnet-mask* {**summarylink** |
nssaexternallink}

- *area-id* — Identifies the OSPF NSSA to configure. (Range: IP address or decimal from 0–4294967295)
- *ip-address* — IP address.
- *subnet-mask* — Subnet mask associated with IP address.
- **summarylink** — Specifies a summary link LSDB type.
- **nssaexternallink** — Specifies an NSSA external link LSDB type.
- **advertise** — Advertisement of the area range.
- **not-advertise** — Suppresses advertisement of the area range.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

Use this command with Area Border Routers (ABRs).

Example

The following example defines an area range for the area 20.

```
console(config-router)#area 20 range 192.168.6.0  
255.255.255.0 summarylink advertise
```

area stub

Use the **area stub** command in Router OSPF Configuration mode to create a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS

External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area. Use the no form of the command to remove the stub area.

Syntax

area *area-id* **stub**

no area *area-id* **stub**

- *area-id* — Identifies the area identifier of the OSPF stub. (Range: IP address or decimal from 0–4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Examples

The following examples define area 3 for the stub and then removes the stub area.

```
console(config-router)#area 3 stub
```

```
console(config-router)#no area 3 stub
```

area stub no-summary

Use the **area stub no-summary** command in Router OSPF Configuration mode to prevent Summary LSAs from being advertised into the NSSA. Use the no form of the command to return the Summary LSA mode to the default value.

Syntax

area *area-id* **stub no-summary**

no area *area-id* stub no-summary

- *area-id*— Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)

Default Configuration

Disabled is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example prevents the Summary LSA from being advertised into the area 3 NSSA.

```
console(config-router)#area 3 stub no-summary
```

area virtual-link

Use the **area virtual-link** command in Router OSPF Configuration mode to create the OSPF virtual interface for the specified area-id and neighbor router. To remove the link, use the no form of the command.

Syntax

area *area-id* virtual-link *neighbor-id*

no area *area-id* virtual-link *neighbor-id*

- *area-id*— Identifies the OSPF area to configure. (Range: IP address or decimal from 0–65535)
- *neighbor-id*— Valid IP address.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example creates an OSPF virtual interface for area 10 and neighbor router.

```
console(config-router)#area 10 virtual-link  
192.168.2.2
```

area virtual-link authentication

Use the **area virtual-link authentication** command in Router OSPF Configuration mode to configure the authentication type and key for the OSPF virtual interface identified by the area ID and neighbor ID. Use the **no** form of the command to return the authentication type to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **authentication** {**none** | **simple** *key* | **encrypt** *key* *key-id*}

no area *area-id* **virtual-link** *neighbor-id* **authentication**

- *area-id* — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
- *neighbor-id* — Identifies the Router identifier of the neighbor.
- **encrypt** — Use MD5 Encryption for an OSPF Virtual Link.
- *key* — Authentication key for the specified interface. (Range: 8 bytes or less if the authentication type is simple and 16 bytes or less if the type is encrypt.)
- *key-id* — Authentication key identifier for the authentication type encrypt. (Range: 0–255)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

Unauthenticated interfaces do not need an authentication key.

Example

The following example configures the authentication type and key for the area 10 OSPF virtual interface and neighbor ID.

```
console(config-router)#area 10 virtual-link  
192.168.2.2 authentication encrypt test123 100
```

area virtual-link dead-interval

Use the **area virtual-link dead-interval** command in Router OSPF Configuration mode to configure the dead interval for the OSPF virtual interface on the virtual interface identified by area-id and neighbor router. Use the no form of the command to return the dead interval to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **dead-interval** *seconds*

no area *area-id* **virtual-link** *neighbor-id* **dead-interval**

- *area-id* — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
- *neighbor-id* — Identifies the Router ID of the neighbor.
- *seconds* — Number of seconds to wait before the OSPF virtual interface on the virtual interface is assumed to be dead. (Range: 1–2147483647)

Default Configuration

40 seconds is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the dead interval for the area 10 OSPF virtual interface on the virtual interface and neighbor router.

```
console(config-router)#area 10 virtual-link  
192.168.2.2 dead-interval 655555
```

area virtual-link hello-interval

Use the **area virtual-link hello-interval** command in Router OSPF Configuration mode to configure the hello interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the hello interval to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **hello-interval** *seconds*

no area *area-id* **virtual-link** *neighbor-id* **hello-interval**

- *area-id* — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
- *neighbor-id* — Identifies the Router ID of the neighbor.
- *seconds* — Number of seconds to wait before sending hello packets to the OSPF virtual interface. (Range: 1–65535)

Default Configuration

10 seconds is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a 50-second wait interval.

```
console(config-router)#area 10 virtual-link  
192.168.2.2 hello-interval 50
```

area virtual-link retransmit-interval

Use the **area virtual-link retransmit-interval** command in Router OSPF Configuration mode to configure the retransmit interval for the OSPF virtual interface on the virtual interface identified by the area ID and neighbor ID. Use the no form of the command to return the retransmit interval to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **retransmit-interval** *seconds*

no area *area-id* **virtual-link** *neighbor-id* **retransmit-interval**

- *area-id*— Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
- *neighbor-id*— Identifies the Router ID of the neighbor.
- *seconds*— The number of seconds to wait between retransmitting LSAs if no acknowledgement is received. (Range: 0–3600)

Default Configuration

The default configuration is 5 seconds.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a 500-second retransmit wait interval.

```
console(config-router)#area 10 virtual-link  
192.168.2.2 retransmit-interval 500
```

area virtual-link transmit-delay

Use the **area virtual-link transmit-delay** command in Router OSPF Configuration mode to configure the transmit delay for the OSPF virtual interface identified by the area ID and neighbor ID. Use the **no** form of the command to return the transmit delay to the default value.

Syntax

area *area-id* **virtual-link** *neighbor-id* **transmit-delay** *seconds*

no area *area-id* **virtual-link** *neighbor-id* **transmit-delay**

- *area-id* — Identifies the OSPF area to configure. (Range: IP address or decimal from 0–4294967295)
- *neighbor-id* — Identifies the Router ID of the neighbor.
- *seconds* — Number of seconds to increment the age of the LSA before sending, based on the estimated time it takes to transmit from the interface. (Range: 0–3600)

Default Configuration

1 second is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a 40-second transmit-delay interval.

```
console(config-router)#area 10 virtual-link  
192.168.2.2 transmit-delay 40
```

auto-cost

By default, OSPF computes the link cost of each interface from the interface bandwidth. The link cost is computed as the ratio of a “reference bandwidth” to the interface bandwidth ($\text{ref_bw} / \text{interface bandwidth}$), where interface bandwidth is defined by the “bandwidth” command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. To change the reference bandwidth, use the auto-cost command, specifying the reference bandwidth in megabits per second. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

Syntax

auto-cost reference-bandwidth *ref_bw*

- *ref_bw*— The reference bandwidth in Mbps (Range: 1–4294967).

Default Configuration

The default reference bandwidth is 100 Mbps.

Command Mode

OSPFv2 or OSPFv3 Router Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example configures a reference bandwidth of 500 Mbps.

```
console(config-router)#auto-cost reference-bandwidth 500
```

bandwidth

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the `auto-cost` command. For the purpose of the OSPF link cost calculation, the `bandwidth` command specifies the interface bandwidth. The bandwidth is specified in kilobits per second. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface.

Syntax

`bandwidth bw`

- *bw* — Interface bandwidth in Kbps (Range: 1–10000000).

Default Configuration

The default reference bandwidth is 10 Mbps

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the interface bandwidth to 500000 Kbps.

```
console (config-if-vlan1) #bandwidth 500000
```

capability opaque

Use the `capability opaque` command to enable Opaque Capability on the router. Use the “no” form of this command to disable Opaque Capability.

Syntax

`capability opaque`

no capability opaque

Default Configuration

Opaque Capability is enabled by default.

Command Mode

Router Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-router)#capability opaque
```

clear ip ospf

Use the **clear ip ospf** command to reset specific OSPF states. If no parameters are specified, OSPF is disabled and then re-enabled.

Syntax

```
clear ip ospf [ { configuration | redistribution | counters | neighbor [ interface vlan vlan id [ neighbor id ] ] } ]
```

- **configuration** — Reset the OSPF configuration to factory defaults.
- **redistribution** — Flush all self-originated external LSAs. Reapply the redistribution configuration and re originate prefixes as necessary.
- **counters** — Reset global and interface statistics.
- **neighbor** — Drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello. Adjacencies may then be reestablished.
- **interface vlan *vlan-id*** — Drop adjacency with all neighbors on a specific interface.
- ***neighbor-id*** — Drop adjacency with a specific router ID on a specific interface.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example shows the options for the **clear ip ospf** command.

```
console#clear ip ospf ?
```

<cr>	Press enter to execute the command.
configuration	Restore OSPF configuration to defaults
counters	Clear OSPF counters
neighbor	Bounce all OSPF neighbors
redistribution	Flush and reoriginate external LSAs

default-information originate

Use the **default-information originate** command in Router OSPF Configuration mode to control the advertisement of default routes. Use the **no** form of the command to return the default route advertisement settings to the default value.

Syntax

default-information originate [*always*] [*metric integer*] [*metric-type* {1|2}]

no default-information originate [*metric*] [*metric-type*]

- *always* — Always advertise default routes.
- *integer* — The metric (or preference) value of the default route. (Range: 1–16777214)
- 1 — External type-1 route.
- 2 — External type-2 route.

Default Configuration

The default metric is none and the default type is 2.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example always advertises default routes.

```
console(config-router)#default-information originate  
always metric 100 metric-type 1
```

default-metric

Use the **default-metric** command in Router OSPF Configuration mode to set a default for the metric of distributed routes. Use the no form of the command to remove the metric from the distributed routes.

Syntax

default-metric *integer*

no default-metric

- *integer* — The metric (or preference) value of the default route. (Range: 1–16777214)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets a value of 50 for the default metric.

```
console (config-router) #default-metric 50
```

distance ospf

The **distance ospf** command sets the preference values of OSPF route types in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, external. All the external type routes are given the same preference value. Use the “no” form of this command to reset the preference values to the default.

Syntax

distance ospf {external | inter-area | intra-area } *distance*

no distance ospf {external | inter-area | intra-area } *distance*

- *distance* — Used to select the best path when there are two or more routes to the same destination from two different routing protocols (Range: 1–255).

Default Configuration

The default preference value is 110.

Command Mode

Router OSPF Configuration mode.

Router OSPFv3 Configuration mode.

User Guidelines

There are no user guidelines for this command.

Examples

The following examples set route preference values of OSPF in the router.

```
console (config-router) #distance ospf intra 4
```

```
console (config-router) #distance ospf type1 19
```

distribute-list out

Use the **distribute-list out** command in Router OSPF Configuration mode to specify the access list to filter routes received from the source protocol. Use the no form of the command to remove the specified source protocol from the access list.

Syntax

distribute-list *accesslistname* **out** {**rip**|**static** |**connected**}

no distribute-list *accesslistname* **out** {**rip**|**static** |**connected**}

- *accesslistname* — The name used to identify an existing ACL. The range is 1–31 characters.
- **rip** — Apply the specified access list when RIP is the source protocol.
- **static** — Apply the specified access list when packets come through the static route.
- **connected** — Apply the specified access list when packets come from a directly connected route.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example specifies the access list to filter routes received from the RIP source protocol.

```
console(config-router)#distribute-list ACL40 out rip
```

enable

Use the **enable** command in Router OSPF Configuration mode to reset the default administrative mode of OSPF in the router (active). Use the no form of the command to disable the administrative mode for OSPF.

Syntax

enable

no enable

Default Configuration

Enabled is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example enables OSPF router mode.

```
console (config-router) #enable
```

exit-overflow-interval

Use the **exit-overflow-interval** command in Router OSPF Configuration mode to configure the exit overflow interval for OSPF. When a router leaves the overflow state it can originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted. Use the no form of the command to return the interval to the default value.

Syntax

exit-overflow-interval *seconds*

no exit-overflow-interval

- *seconds* — Number of seconds after entering overflow state that a router will wait before attempting to leave the overflow state. (Range: 0–2147483647)

Default Configuration

0 seconds is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the exit overflow interval for OSPF at 10 seconds.

```
console(config-router)#exit-overflow-interval 10
```

external-lsdb-limit

Use the **external-lsdb-limit** command in Router OSPF Configuration mode to configure the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in its database. Use the **no** form of the command to return the limit to the default value.

Syntax

external-lsdb-limit *integer*

no external-lsdb-limit

- *integer* — Maximum number of non-default AS-external-LSAs allowed in the router's link-state database. (Range: -1 to 2147483647)

Default Configuration

-1 is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

The external LSDB limit **MUST** be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area.

Example

The following example configures the external LSDB limit for OSPF with the number of non-default AS external-LSAs set at 20.

```
console(config-router)#external-lsdb-limit 20
```

ip ospf area

The **ip ospf area** command enables OSPFv2 and sets the area ID of an interface. This command supersedes the effects of network area command. It can also configure the advertisability of the secondary addresses on this interface into OSPFv2 domain. Use the “no” form of this command to disable OSPFv2 on an interface.

Syntax

ip ospf area *area-id* [secondaries none]

no ip ospf area [secondaries none]

- *area-id* — The ID of the area (Range: IP address or decimal from 0 –4294967295).

Default Configuration

OSPFv2 is disabled by default.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan1)#ip ospf area 192.168.1.10
```

ip ospf authentication

Use the **ip ospf authentication** command in the Interface Configuration mode to set the OSPF Authentication Type and Key for the specified interface. Use the **no** form of the command to return the authentication type to the default value.

Syntax

ip ospf authentication {none | {simple *key*} | {encrypt *key key-id*}}

no ip ospf authentication

- **encrypt** — MD5 encrypted authentication key.
- *key* — Authentication key for the specified interface. (Range: 8 bytes or less if the authentication type is **simple** and 16 bytes or less if the type is **encrypt**.)
- *key-id* — Authentication key identifier for the authentication type **encrypt**. (Range: 0–25)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

Unauthenticated interfaces do not need an authentication key or authentication key ID.

Example

The following example sets the OSPF Authentication Type and Key for VLAN 15.


```
console(config-if-vlan15)#ip ospf authentication
encrypt test123 100
```

ip ospf cost

Use the **ip ospf cost** command in Interface Configuration mode to configure the cost on an OSPF interface. Use the no form of the command to return the cost to the default value.

Syntax

```
ip ospf cost integer
```

```
no ip ospf cost
```

- *integer*— Specifies the cost (link-state metric) of the OSPF interface. (Range: 1–65535)

Default Configuration

10 is the default link-state metric configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the cost on the OSPF interface at 5.

```
console(config-if-vlan15)#ip ospf cost 5
```

ip ospf dead-interval

Use the **ip ospf dead-interval** command in Interface Configuration to set the OSPF dead interval for the specified interface. Use the no form of the command to return the interval to the default value.

Syntax

`ip ospf dead-interval seconds`

`no ip ospf dead-interval`

- *seconds* — Number of seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. (Range: 1–65535)

Default Configuration

40 is the default number of seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4).

Example

The following example sets the dead interval at 30 seconds.

```
console(config-if-vlan15)#ip ospf dead-interval 30
```

ip ospf hello-interval

Use the `ip ospf hello-interval` command in Interface Configuration mode to set the OSPF hello interval for the specified interface. Use the `no` form of the command to return the interval to the default value.

Syntax

`ip ospf hello-interval seconds`

`no ip ospf hello-interval`

- *seconds* — Number of seconds to wait before sending Hello packets from the interface. (Range: 1–65535)

Default Configuration

10 is the default number of seconds.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

The value for the length of time must be the same for all routers attached to a network.

Example

The following example sets the OSPF hello interval at 30 seconds.

```
console(config-if-vlan15)#ip ospf hello-interval 30
```

ip ospf mtu-ignore

Use the **ip ospf mtu-ignore** command in Interface Configuration mode to disable OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established. Use the **no** form of the command to enable OSPF maximum transmission unit (MTU) mismatch detection.

Syntax

```
ip ospf mtu-ignore
```

```
no ip ospf mtu-ignore
```

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example disables OSPF MTU mismatch detection on VLAN interface 15.

```
console(config-if-vlan15)#ip ospf mtu-ignore
```

ip ospf network

Use the **ip ospf network** command to configure OSPF to treat an interface as a point-to-point rather than broadcast interface. To return to the default value, use the **no** form of this command.

Syntax

```
ip ospf network { broadcast | point-to-point }
```

```
no ip ospf network
```

- *broadcast* — Set the network type to broadcast.
- *point-to-point* — Set the network type to point-to-point

Default Configuration

Interfaces operate in broadcast mode by default.

Command Mode

Interface Configuration (VLAN) mode.

Usage Guidelines

OSPF treats interfaces as broadcast interfaces by default. Loopback interfaces have a special loopback network type, which cannot be changed. When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.

Example

The following example shows the options for the **ip ospf network** command.

```
console(config-if-vlan1)#ip ospf network ?
```

broadcast	Set the OSPF network type to Broadcast
point-to-point	Set the OSPF network type to Point-to-Point

ip ospf priority

Use the **ip ospf priority** command in Interface Configuration mode to set the OSPF priority for the specified router interface. Use the **no** form of the command to return the priority to the default value.

Syntax

ip ospf priority *integer*

no ip ospf priority

- *integer* — Specifies the OSPF priority for the specified router interface. (Range: 0–255)

Default Configuration

1 is the default integer value.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

A value of 1 is the highest router priority. A value of 0 indicates that the interface is not eligible to become the designated router on this network.

Example

The following example sets the OSPF priority for the VLAN 15 router at 100.

```
console(config-if-vlan15)#ip ospf priority 100
```

ip ospf retransmit-interval

Use the **ip ospf retransmit-interval** command in Interface Configuration mode to set the OSPF retransmit Interval for the specified interface. Use the no form of the command to return the interval to the default value.

Syntax

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

- *seconds* — Number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. (Range: 0–3600 seconds)

Default Configuration

5 is the default number of seconds.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

A value of 1 is the highest router priority. A value of 0 indicates that the interface is not eligible to become the designated router on this network.

Example

The following example sets the OSPF retransmit Interval for VLAN 15 at 50 seconds.

```
console(config-if-vlan15)#ip ospf retransmit-interval 50
```

ip ospf transmit-delay

Use the **ip ospf transmit-delay** command in Interface Configuration mode to set the OSPF Transit Delay for the specified interface. Use the no form of the command to return the delay to the default value.

Syntax

`ip ospf transmit-delay seconds`

`no ip ospf transmit-delay`

- *seconds*— Sets the estimated number of seconds it takes to transmit a link state update packet over this interface. (Range: 1–3600 seconds)

Default Configuration

1 is the default number of seconds.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF Transit Delay for VLAN 15 at 20 seconds.

```
console(config-if-vlan15)#ip ospf transmit-delay 20
```

maximum-paths

Use the **maximum-paths** command in Router OSPF Configuration mode to set the number of paths that OSPF can report for a given destination. Use the `no` form of the command to reset the number to the default value.

Syntax

`maximum-paths integer`

`no maximum-paths`

- *integer*— Number of paths that OSPF can report for a given destination. (Range: 1–4.)

Default Configuration

4 is the *integer* default value.

Command Mode

Router OSPF Configuration mode.

User Guidelines

OSPF is only enabled on an interface if the primary IPv4 address on the interface matches a network area range. Any individual interface can only be attached to a single area. If an interface address matches multiple network area ranges, the interface is assigned to the area for the first matching range. If the **ip ospf area** command is given for an interface, it overrides any matching network area command.

OSPF only advertises IP subnets for secondary IP addresses if the secondary address is within the range of a network area command for the same area as the primary address on the same interface.

When a network area command is deleted, matching interfaces are reevaluated against all remaining network area commands.

Example

The following example sets the number of paths at 2 that OSPF can report for a given destination.

```
console(config-router)#maximum-paths 2
```

network area

The **network area** command enables OSPFv2 on an interface and sets its area ID if the ip-address of an interface is covered by this network command. Use the “no” form of this command to disable OSPFv2 on an interface.

Syntax

network *ip-address wildcard-mask* **area** *area-id*

no network *ip-address wildcard-mask* **area** *area-id*

- *ip-address* — Base IPv4 address of the network area.
- *wildcard-mask* — The network mask indicating the subnet.
- *area-id* — The ID of the area (Range: IP address or decimal from 0–4294967295).

Default Configuration

OSPFv2 is disabled

Command Mode

Router OSPF Configuration mode.

User Guidelines

OSPF is only enabled on an interface if the primary IPv4 address on the interface matches a network area range. Any individual interface can only be attached to a single area. If an interface address matches multiple network area ranges, the interface is assigned to the area for the first matching range. If the **ip ospf area** command is given for an interface, it overrides any matching network area command.

OSPF only advertises IP subnets for secondary IP addresses if the secondary address is within the range of a network area command for the same area as the primary address on the same interface.

When a network area command is deleted, matching interfaces are reevaluated against all remaining network area commands.

Example

```
console(config-router)#network 10.50.50.0 0.0.0.255  
area 4
```

nsf

Use this command to enable OSPF graceful restart. Use the “no” form of this command to disable graceful restart.

Syntax

```
nsf [ ietf ] [ planned-only ]
```

```
no nsf [ ietf ]
```

ietf — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.

planned-only — This keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).

Default Configuration

Graceful restart is disabled by default

Command Mode

Router OSPF Configuration mode

User Guidelines

Graceful restart works in concert with nonstop forwarding to enable the hardware to continue forwarding IPv4 packets using OSPFv2 routes while a backup unit takes over management unit responsibility. When OSPF executes a graceful restart, it informs its neighbors that the OSPF control plane is restarting, but that it will be back shortly. Helpful neighbors continue to advertise to the rest of the network that they have full adjacencies with the restarting router, avoiding announcement of a topology change and everything that goes with that (i.e., flooding of LSAs, SPF runs). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

This implementation of graceful restart restarting router behavior is only useful with a router stack. Graceful restart does not work on a standalone, single-unit router.

Example

—

nsf helper

Use the **nsf-helper** to allow OSPF to act as a helpful neighbor for a restarting router. Use the “no” form of this command to prevent OSPF from acting as a helpful neighbor.

Syntax

nsf helper[planned-only]

no nsf helper

- **planned-only** — This keyword indicates that OSPF should only help a restarting router performing a planned restart.

Default Configuration

OSPF may act as a helpful neighbor for both planned and unplanned restarts

Command Mode

Router OSPF Configuration mode

User Guidelines

The grace LSA announcing the graceful restart includes a restart reason. Reasons 1 (software restart) and 2 (software reload/upgrade) are considered planned restarts. Reasons 0 (unknown) and 3 (switch to redundant control processor) are considered unplanned restarts.

nsf ietf helper disable is functionally equivalent to **no nsf helper** and is supported solely for IS CLI compatibility.

Example

—

nsf helper strict-lsa-checking

Use the **nsf-helper strict-lsa-checking** command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs. Use the “no” form of this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Syntax

nsf [ietf] helper strict-lsa-checking

no nsf [ietf] helper strict-lsa-checking

- **ietf** —This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.

Default Configuration

A helpful neighbor exits helper mode when a topology change occurs.

Command Mode

Router OSPF Configuration mode

User Guidelines

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router.

A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Example

—

nsf restart-interval

Use the **nsf restart-interval** command to configure the length of the grace period on the restarting router. Use the “no” form of this command to revert the grace period to its default.

Syntax

nsf [**ietf**] **restart-interval** *seconds*

no nsf [**ietf**] **restart-interval**

- **ietf** — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.
- *seconds* — The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The restarting router includes the restart interval in its grace LSAs (range 1–1800 seconds).

Default Configuration

The default restart interval is 120 seconds.

Command Mode

Router OSPF

User Guidelines

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Example

—

passive-interface default

The **passive-interface default** command enables the global passive mode by default for all interfaces. It overrides any interface level passive mode. Use the “no” form of this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Syntax

passive-interface default

no passive-interface default

Default Configuration

Global passive mode is disabled by default.

Command Mode

Router OSPF Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-router)#passive-interface
```

passive-interface

Use the **passive-interface** command to set the interface as passive. It overrides the global passive mode that is currently effective on the interface. Use the “no” form of this command to set the interface as non-passive.

Syntax

```
passive-interface vlan vlan-id  
no passive-interface vlan vlan-id
```

- *vlan-id* — The vlan number

Default Configuration

Passive interface mode is disabled by default.

Command Mode

Router OSPF Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-router)#passive-interface vlan 1
```

redistribute

Use the **redistribute** command in Router OSPF Configuration mode to configure OSPF protocol to allow redistribution of routes from the specified source protocol/routers. Use the no version of the command to disable redistribution from the selected source or to reset options to their default values.

Syntax

`redistribute {rip | static | connected} [metric integer] [metric-type {1 | 2}] [tag integer] [subnets]`

`no redistribute {rip | static | connected} [metric integer] [metric-type {1 | 2}] [tag integer] [subnets]`

- **rip** — Specifies RIP as the source protocol.
- **static** — Specifies that the source is a static route.
- **connected** — Specifies that the source is a directly connected route.
- **metric** — Specifies the metric to use when redistributing the route. (Range: 0–16777214)
- **metric-type 1** — Type 1 external route.
- **metric-type 2** — Type 2 external route.
- **tag** — Value attached to each external route, which might be used to communicate information between ASBRs. (Range: 0–4294967295)
- **subnets** — Specifies whether to redistribute the routes to subnets.

Default Configuration

0 is the tag integer default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

```
console(config-router)#redistribute rip metric 90
metric-type 1 tag 555 subnets
```

router-id

Use the **router-id** command in Router OSPF Configuration mode to set a 4-digit dotted-decimal number uniquely identifying the router OSPF ID.

Syntax

router-id *ip-address*

- *ip-address* — IP address that uniquely identifies the router OSPF ID.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example defines the router OSPF ID as 5.5.5.5.

```
console(config)#router ospf
console(config-router)#router-id 5.5.5.5
```

router ospf

Use the **router ospf** command in Global Configuration mode to enter Router OSPF mode.

Syntax

router ospf

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode.

User Guidelines

The command prompt changes when the **router ospf** command executes.

Example

The following example enters into router OSPF mode.

```
console(config)#router ospf
console(config-router)#
```

show ip ospf

Use the **show ip ospf** command to display information relevant to the OSPF router. This command has been modified to show additional fields.

Syntax

show ip ospf

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

Some of the information below displays only if you enable OSPF and configure certain features. The following fields may be displayed:

Router ID	A 32-bit integer in dotted decimal format identifying the router about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether OSPF is administratively enabled or disabled.

RFC 1583 Compatibility	This configuration option controls the preference rules used when choosing among multiple external LSAs advertising the same destination. When enabled, the preference rules remain those specified by RFC 1583. When disabled, the preference rules are those stated in Section 16.4.1 of RFC 2328. These rules prevent routing loops when external LSAs for the same destination have been originated from different areas.
External LSDB Limit	Shows the maximum number of non-default external LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	Shows the number of seconds that, after entering OverflowState, as defined by RFC 1765, a router will attempt to leave OverflowState.
Spf Delay Time	The number of seconds to wait before running a routing table calculation after a topology change.
Spf Hold Time	The minimum number of seconds between routing table calculations.
Opaque Capability	Shows whether router is capable of sending Opaque LSAs.
AutoCost Ref BW	The configured autcost reference bandwidth. This value is used to determine the OSPF metric on its interfaces. The reference bandwidth is divided by the interface speed to compute the metric.
Default Passive Setting	When enabled, OSPF interfaces are passive by default.
Maximum Paths	Shows the maximum number of paths that OSPF can report for a given destination.
Default Metric	Default metric for redistributed routes.
Default Route Advertise	When enabled, OSPF originates a type 5 LSA advertising a default route.
Always	When this option is configured, OSPF only originates a default route when the router has learned a default route from another source.
Metric	Shows the metric for the advertised default routes. If the metric is not configured, this field is not configured.
Metric Type	Shows whether the metric for the default route is advertised as External Type 1 or External Type 2.

Number of Active Areas	The number of OSPF areas to which the router is attached on interfaces that are up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	Indicates whether the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learned from another protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router	OSPF enters stub router mode, as described in RFC 3137, when it encounters a resource limitation that prevents it from computing a complete routing table. In this state, OSPF sets the link metrics of non-stub links in its own router LSAs to the largest possible value, discouraging other routers from computing paths through the stub router, but allowing other routers to compute routes to destinations attached to the stub router. To restore OSPF to normal operation, resolve the condition that caused the resource overload, then disable and re-enable OSPF globally.
External LSDB Overflow	OSPF enters this state when the number of external LSAs exceeds a configured limit, as described in RFC 1765.
External LSA Count	Shows the number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.
AS_OPAQUE LSA Count	Shows the number of AS Opaque LSAs received.
AS_OPAQUE LSA Checksum	Sum of the checksums of all AS Opaque LSAs in the link state database.
New LSAs Originated	Shows the number of link-state advertisements that have been originated.
LSAs Received	Shows the number of link-state advertisements received determined to be new instantiations.
LSA Count	The number of LSAs in the link state database.
Maximum Number of LSAs	The limit on the number of LSAs that the router can store in its link state database.

LSA High Water Mark	The maximum number of LSAs that have been in the link state database since OSPF began operation.
Retransmit List Entries	The current number of entries on all neighbors' retransmit lists.
Maximum Number of Retransmit Entries	The maximum number of entries that can be on neighbors' retransmit lists at any given time. This is the sum for all neighbors. When OSPF receives an LSA and cannot allocate a new retransmit list entry, the router does not acknowledge the LSA, expecting the sender to retransmit.
Retransmit Entries High Water Mark	The maximum number of retransmit list entries that have been on all neighbors' retransmit lists at one time.
NSF Support	Whether graceful restart is administratively enabled. Possible values are Support Always, Disabled, or Planned.
NSF Restart Interval	The number of seconds a helpful neighbor allows a restarting router to complete its graceful restart.
NSF Restart Status	Whether the router is currently performing a graceful restart.
NSF Restart Age	The number of seconds until a graceful restart expires. Only non-zero when the router is in graceful restart.
NSF Restart Exit Reason	The reason the previous graceful restart ended. Possible values are Not attempted, In progress, Completed, Timed out, Topology change, and Manual clear.
NSF Helper Support	Whether this router is configured to act as a graceful restart helpful neighbor. Possible values are: Helper Support Always, Disabled, or Planned.
NSF Helper Strict LSA Checking	As a graceful restart helpful neighbor, whether to terminate the helper relationship if a topology change occurs during a neighbor's graceful restart.
Redistributing	This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.
Source	Shows source protocol/routes that are being redistributed. Possible values are static, connected, or RIP.
Tag	Shows the decimal value attached to each external route.
Subnets	When this option is not configured, OSPF will only redistribute classful prefixes.

Distribute-List	Shows the access list used to filter redistributed routes.
-----------------	--

Example

The following example displays OSPF router information.

```
console#show ip ospf
```

```
Router ID..... 1.1.1.1
OSPF Admin Mode..... Enable
RFC 1583 Compatibility..... Enable
External LSDB Limit..... No Limit
Exit Overflow Interval..... 0
Spf Delay Time..... 5
Spf Hold Time..... 10
Opaque Capability..... Disable
AutoCost Ref BW..... 100 Mbps
Default Passive Setting..... Disabled
Maximum Paths..... 4
Default Metric..... Not
configured

Default Route Advertise..... Disabled
Always..... FALSE
Metric..... Not
configured
Metric Type..... External
Type 2

Number of Active Areas..... 1 (1 normal,
0 stub, 0 nssa)
ABR Status..... Disable
```

ASBR Status.....	Disable
Stub Router.....	FALSE
External LSDB Overflow.....	FALSE
External LSA Count.....	0
External LSA Checksum.....	0
AS_OPAQUE LSA Count.....	0
AS_OPAQUE LSA Checksum.....	0
New LSAs Originated.....	25
LSAs Received.....	7
LSA Count.....	4
Maximum Number of LSAs.....	18200
LSA High Water Mark.....	4
Retransmit List Entries.....	0
Maximum Number of Retransmit Entries.....	72800
Retransmit Entries High Water Mark.....	2
NSF Support.....	Disabled
NSF Restart Interval.....	120
NSF Restart Status.....	Not
Restarting	
NSF Restart Age.....	0 seconds
NSF Restart Exit Reason.....	Not
Attempted	
NSF Helper Support.....	Always
NSF Helper Strict LSA Checking.....	Enabled

show ip ospf abr

The `show ip ospf abr` command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options.

Syntax

`show ip ospf abr`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show ip ospf abr
```

Type	Router Id	Cost	Area ID	Next Hop	NextHop Intf
-----	-----	-----	-----	-----	-----
INTRA	3.3.3.3	1	0.0.0.1	10.1.23.3	vlan11
INTRA	4.4.4.4	10	0.0.0.1	10.1.24.4	vlan12

show ip ospf area

Use the `show ip ospf area` command in Privileged EXEC mode to display information about the identified OSPF area.

Syntax

`show ip ospf area area-id`

- *area-id* — Identifies the OSPF area whose ranges are being displayed. (Range: 0–4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays OSPF router information.

```
console#show ip ospf area 10
AreaID..... 0.0.0.10
External Routing..... Import
External LSAs
Spf Runs..... 0
Area Border Router Count..... 0
Area LSA Count..... 0
Area LSA Checksum..... 0
Import Summary LSAs..... Enable
console#show ip ospf area 20
AreaID..... 0.0.0.20
External Routing..... Import NSSAs
Spf Runs..... 0
Area Border Router Count..... 0
Area LSA Count..... 0
Area LSA Checksum..... 0
OSPF NSSA Specific Information.
Import Summary LSAs..... Enable
Redistribute into NSSA..... Enable
Default Information Originate..... TRUE
```



```
Default Metric..... 250
Default Metric Type..... Non-Comparable
Translator Role..... Candidate
Translator Stability Interval..... 2000
Translator State..... Disabled
```

show ip ospf asbr

The **show ip ospf asbr** command displays the internal OSPF routing table entries to Autonomous System Boundary Routes (ASBR). This command takes no options.

Syntax

```
show ip ospf asbr
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

```
console#show ip ospf asbr
```

Type	Router Id	Cost	Area ID	Next Hop	Next Hop Intf
-----	-----	----	-----	-----	-----
INTRA	1.1.1.1	1	0.0.0.1	10.1.12.1	vlan10
INTRA	4.4.4.4	10	0.0.0.1	10.1.24.4	vlan12

show ip ospf database

Use the **show ip ospf database** command in Privileged EXEC mode to display information about the link state database when OSPF is enabled. If parameters are entered, the command displays the LSA headers. Use the optional parameters to specify the type of link state advertisements to display.

Syntax

show ip ospf [*<area-id>*] **database** [{**asbr-summary** | **external** | **network** | **nssa-external** | **router** | **summary**}] [*ls-id*] [**adv-router** *ip-address*] | **self-originate**]

- *area-id* — Identifies a specific OSPF area for which link state database information will be displayed.
- **asbr-summary** — Display the autonomous system boundary router (ASBR) summary LSAs.
- **external** — Display the external LSAs.
- **network** — Display the network LSAs.
- **nssa-external** — Display NSSA external LSAs.
- **router** — Display router LSAs.
- **summary** — Display the LSA database summary information.
- *ls-id* — Specifies the link state ID (LSID). (Range: IP address or an integer in the range of 0–4294967295)
- **adv-router** — Display the LSAs that are restricted by the advertising router. To specify a router, enter the IP address of the router.
- **self-originate** — Display the LSAs in that are self-originated.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

Information is only displayed if OSPF is enabled.

Example

The following example displays information about the link state database when OSPF is enabled.

console#show ip ospf database

Router Link States (Area 0.0.0.0)						
Link Id	Adv Router	Age	Sequence Chksm	Options	Rtr Opt	
5.2.0.0	0.0.0.0	1360	80000006 3a1f	-----	-----	
5.2.0.0	5.2.0.0	1360	80000009 a47e	-----	---E-	
20.20.20.20	20.20.20.20	1165	8000000b 0f80	-E----	-----	
Network Link States (Area 0.0.0.0)						
Link Id	Adv Router	Age	Sequence Chksm	Options	Rtr Opt	
2.2.2.2	20.20.20.20	1165	80000005 f86d	-E--O-		
Network Summary States (Area 0.0.0.0)						
Link Id	Adv Router	Age	Sequence Chksm	Options	Rtr Opt	
5.2.0.0	0.0.0.0	1360	80000007 242e	-----		
Summary ASBR States (Area 0.0.0.0)						
Link Id	Adv Router	Age	Sequence Chksm	Options	Rtr Opt	
5.2.0.0	0.0.0.0	1361	80000006 183a	-----		

Link Opaque States (Area 0.0.0.0)

Link Id	Adv Router	Age	Sequence	Chksm	Options	Rtr Opt
5.2.0.0	0.0.0.0	1361	80000005	ef59	-----	

Area Opaque States (Area 0.0.0.0)

Link Id	Adv Router	Age	Sequence	Chksm	Options	Rtr Opt
5.2.0.0	0.0.0.0	1362	80000005	e166	-----	

AS External States

Link Id	Adv Router	Age	Sequence	Chksm	Options	Rtr Opt
6.0.0.0	5.2.0.0	1364	80000008	e35d		

AS Opaque States

Link Id	Adv Router	Age	Sequence	Chksm	Options	Rtr Opt
5.2.0.0	0.0.0.0	1364	80000005	d373		

show ip ospf database database-summary

Use the **show ip ospf database database-summary** command to display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database. This command has been modified.

Syntax

show ip ospf database database-summary

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

The following fields are displayed:

Router	Shows Total number of router LSAs in the OSPF link state database.
Network	Shows Total number of network LSAs in the OSPF link state database.
Summary Net	Shows Total number of summary network LSAs in the database.
Summary ASBR	Shows Number of summary ASBR LSAs in the database.
Type-7 Ext	Shows Total number of Type-7 external LSAs in the database.
Self- Originated Type-7	Shows Total number of self originated AS external LSAs in the OSPFv3 link state database.
Opaque Link	Shows Number of opaque link LSAs in the database.
Opaque Area	Shows Number of opaque area LSAs in the database.
Subtotal	Shows Number of entries for the identified area.
Opaque AS	Shows Number of opaque AS LSAs in the database.
Total	Shows Number of entries for all areas.

Example

The following example displays the number of each type of LSA in the database for each area and for the router.

```
console#show ip ospf database database-summary
OSPF Router with ID (5.5.5.5)
Area 0.0.0.0 database summary
Router..... 0
Network..... 0
Summary Net..... 0
Summary ASBR..... 0
Type-7 Ext..... 0
Self Originated Type-7..... 0
Opaque Link..... 0
Opaque Area..... 0
Subtotal..... 0
Area 0.0.0.10 database summary
Router..... 0
Network..... 0
Summary Net..... 0
Summary ASBR..... 0
Type-7 Ext..... 0
Self Originated Type-7..... 0
Opaque Link..... 0
Opaque Area..... 0
Subtotal..... 0
Router database summary
```

Router.....	0
Network.....	0
Summary Net.....	0
Summary ASBR.....	0
Type-7 Ext.....	0
Opaque Link.....	0
Opaque Area.....	0
Type-5 Ext.....	0
Self-Originated Type-5 Ext.....	0
Opaque AS.....	0
Total.....	0

show ip ospf interface

Use the `show ip ospf interface` command in Privileged EXEC mode to display the information for the VLAN or loopback interface.

Syntax

`show ip ospf interface {vlan vlan-id | loopback loopback-id}`

- *vlan-id*— Valid VLAN ID.
- *loopback-id*— Shows information the specified loopback interface.
(Range: 0–7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the information for the IFO object or virtual interface tables associated with VLAN 3.

```
console#show ip ospf interface vlan 10
```

```
IP Address..... 1.1.1.1
Subnet Mask..... 255.255.255.0
Secondary IP Address(es) .....
OSPF Admin Mode..... Enable
OSPF Area ID..... 0.0.0.0
OSPF Network Type..... Broadcast
Router Priority..... 1
Retransmit Interval..... 5
Hello Interval..... 10
Dead Interval..... 40
LSA Ack Interval..... 1
Iftransit Delay Interval..... 1
Authentication Type.....None
Metric Cost.....10 (computed)
Passive Status..... Non-passive interface
OSPF Mtu-ignore..... Disable
State..... .. designated-router
Designated Router..... 1.1.1.1
Backup Designated Router..... 0.0.0.0
Number of Link Events..... 2
```


show ip ospf interface brief

Use the `show ip ospf interface brief` command in Privileged EXEC mode to display brief information for the IFO object or virtual interface tables.

Syntax

`show ip ospf interface brief`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays brief information for the IFO object or virtual interface tables.

```
console#show ip ospf interface brief
Router Hello Dead Retrax Retrax LSAAck
Interface AdminMode AreaID Priority Intval Intval Delay Intval
-----
vlan1      Enable    0.0.0.10 1      10     40     5      1      1
vlan2      Disable   0.0.0.0  1      10     40     5      1      1
vlan3      Disable   0.0.0.0  1      10     40     5      1      1
loopback2  Disable   0.0.0.0  1      10     40     5      1      1
```

show ip ospf interface stats

Use the `show ip ospf interface stats` command in User EXEC mode to display the statistics for a specific interface. The information is only displayed if OSPF is enabled.

Syntax

`show ip ospf interface stats vlan vlan-id`

- *vlan-id*— Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the ospf statistics for VLAN 15.

```
console>show ip ospf interface stats vlan15
OSPF Area ID..... 0.0.0.0
Area Border Router Count..... 0
AS Border Router Count.....0
Area LSA Count......1
IP Address.....2.2.2.2
OSPF Interface Events.....1
Virtual Events..... 0
Neighbor Events..... 0
External LSA Count..... 0
```

show ip ospf neighbor

Use the `show ip ospf neighbor` command in Privileged EXEC mode to display information about OSPF neighbors. The information below only displays if OSPF is enabled and the interface has a neighbor.

Syntax

`show ip ospf neighbor [interface vlan vlan-id] [ip-address]`

- *vlan-id* — Valid VLAN ID.
- *ip-address* — Valid IP address of the neighbor.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following examples display information about OSPF neighbors on the specified Ethernet and IP interfaces.

```
console #show ip ospf neighbor 10.1.23.50
```

```
Interface..... vlan 20
Neighbor IP Address..... 10.1.13.50
Interface Index..... 65
Area Id..... 0.0.0.1
Options..... 0x42
Router Priority..... 1
Dead timer due in (secs)..... 33
Up Time..... 4 days 12 hrs 56 mins 6
secs
State..... Full/DR
Events..... 13
Retransmission Queue Length..... 0
Restart Helper Status..... Helping
Restart Reason..... Software Restart (1)
Remaining Grace Time..... 10 sec
Restart Helper Exit Reason..... In Progress
```

Field Descriptions

Interface — The name of the interface on which the adjacency is formed.

Neighbor IP Address — The IPv4 address on the neighbor's interface used to form the adjacency.

Interface Index — The SNMP interface index.

Area Id — The OSPF area in which the adjacency is formed

Options — The options advertised by the neighbor

Router Priority: The router priority advertised by the neighbor

Dead timer — The number of seconds until the dead timer expires

Up Time — How long this adjacency has been in FULL state

State — The current state of the adjacency

Events: Incremented for the following events:

A DD is received from the neighbor with an MTU mismatch

The neighbor sent an ACK for an LSA not on the neighbor's retransmit list

The state of the adjacency changed.

Retransmission Queue Length — The number of LSAs on the neighbor's retransmit queue waiting for the neighbor to acknowledge.

Restart Helper Status: One of two values:

- Helping — This router is acting as a helpful neighbor to this neighbor. A helpful neighbor does not report an adjacency change during graceful restart, but continues to advertise the restarting router as a FULL adjacency. A helpful neighbor continues to forward data packets to the restarting router, trusting that the restarting router's forwarding table is maintained during the restart.
- Not Helping — This router is not a helpful neighbor at this time.

Restart Helper Exit Reason is one of the following values:

- Restart Reason — When the router is in helpful neighbor mode, the output includes the restart reason the restarting router sent in its grace LSA. The Restart Reason is the value in the Graceful Restart Reason TLV in the grace LSA sent by the restarting router. Possible values for the Restart Reason are defined in RFC 3623 as follows:
 - Unknown (0)

- Software restart (1)
- Software reload/upgrade (2)
- Switch to redundant control processor (3)
- Unrecognized - a value not defined in RFC 3623

When FASTPATH sends a grace LSA, it sets the Restart Reason to Software Restart on a planned warm restart (when the "initiate failover" command is invoked), and to Unknown on an unplanned warm restart.

- Remaining Grace Time — The number of seconds remaining in the current graceful restart interval. This row is only included if the router is currently acting as a restart helper for the neighbor.
- Restart Exit Reason — One of the following:
 - None — graceful restart has not been attempted
 - In Progress — restart is in progress
 - Completed — the previous graceful restart completed successfully
 - Timed Out — the previous graceful restart timed out
 - Topology Changed — The previous graceful restart terminated prematurely because of a topology change. A helpful neighbor declares a topology change when it forwards a changed LSA to the restarting router. An LSA is considered changed if its contents are changed, not if it is simply a periodic refresh.

show ip ospf range

Use the `show ip ospf range` command in Privileged EXEC mode to display information about the area ranges for the specified area-id.

Syntax

`show ip ospf range area-id`

- *area-id*— Identifies the OSPF area whose ranges are being displayed. (Range: IP address or decimal from 0–4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the area ranges for the specified area-id.

```
console#show ip ospf range 20
```

Area ID	IP Address	Subnet Mask	Lsdb Type	Advertisement
-----	-----	-----	-----	-----
0.0.0.20	192.168.6.0	255.255.255.0	Summary Link	Enabled

show ip ospf statistics

This command displays information about recent Shortest Path First (SPF) calculations. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the table lists how long ago the SPF ran, how long the SPF took, and the reasons why the SPF was scheduled.

Syntax

show ip ospf statistics

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

```
console>show ip ospf statistics
Area 0.0.0.0: SPF algorithm executed 0 times
Delta T      SPF Duration (msec)      Reason
-----
26:01:45      0
23:15:05      0      R
23:14:22      0      R, N
23:14:12      0      R
23:10:04      0
```

show ip ospf stub table

Use the **show ip ospf stub table** command in Privileged EXEC mode to display the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Syntax

show ip ospf stub table

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF stub table.

```
console(config)#show ip ospf stub table
AreaId          TypeofService  Metric Val Import SummaryLSA
```

```
-----
0.0.0.1          Normal          1          Enable
```

show ip ospf virtual-link

Use the **show ip ospf virtual-link** command in Privileged EXEC mode to display the OSPF Virtual Interface information for a specific area and neighbor.

Syntax

show ip ospf virtual-link *area-id neighbor-id*

- *area-id*— Identifies the OSPF area whose ranges are being displayed. (Range: IP address or decimal from 0–4294967295)
- *neighbor-id*— Identifies the neighbor's router ID. (Range: Valid IP address)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF Virtual Interface information for area 10 and its neighbor.

```
console#show ip ospf virtual-link 10 192.168.2.2
Area ID..... 10
Neighbor Router ID..... 192.168.2.2
Hello Interval..... 10
Dead Interval..... 655555
Iftransit Delay Interval..... 1
Retransmit Interval..... 5
State..... down
Metric..... 0
Neighbor State..... down
Authentication Type..... MD5
Authentication Key..... "test123"
Authentication Key ID..... 100
```

show ip ospf virtual-link brief

Use the `show ip ospf virtual-link brief` command in Privileged EXEC mode to display the OSPF Virtual Interface information for all areas in the system.

Syntax

`show ip ospf virtual-link brief`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF Virtual Interface information in the system.

```
console#show ipv6 ospf virtual-link brief
```

Area ID	Neighbor	Hello Interval	Dead Interval	Retransmit Interval	Transit Delay
0.0.0.2	5.5.5.5	10	40	5	1

timers spf

Use the **timers spf** command in Router OSPF Configuration mode to configure the SPF delay and hold time. Use the no form of the command to reset the numbers to the default value.

Syntax

timers spf *delay-time* *hold-time*

no timers spf

- *delay-time* — SPF delay time. (Range: 0–65535 seconds)
- *hold-time* — SPF hold time. (Range: 0–65535 seconds)

Default Configuration

The default value for *delay-time* is 5. The default value for *hold-time* is 10.

Command Mode

Router OSPF Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the SPF delay and hold time.

```
console(config-router)#timers spf 20 30
```

1583compatibility

Use the **1583compatibility** command in Router OSPF Configuration mode to enable OSPF 1583 compatibility. Use the **no** form of the command to disable it.

Syntax

1583compatibility

no 1583compatibility

Default Configuration

Enabled is the default configuration.

Command Mode

Router OSPF Configuration mode.

User Guidelines

If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Example

The following example enables 1583 compatibility.

```
console(config-router)#1583compatibility
```


OSPFv3 Commands

This chapter explains the following commands:

- area default-cost
- area nssa
- area nssa default-info-originate
- area nssa no-redistribute
- area nssa no-summary
- area nssa translator-role
- area nssa translator-stab-intv
- area range
- area stub
- area stub no-summary
- area virtual-link
- area virtual-link dead-interval
- area virtual-link hello-interval
- area virtual-link retransmit-interval
- area virtual-link transmit-delay
- default-information originate
- default-metric
- distance ospf
- enable
- exit-overflow-interval
- external-lsdb-limit
- ipv6 ospf
- ipv6 ospf areaid
- ipv6 ospf cost
- ipv6 ospf dead-interval

- ipv6 ospf hello-interval
- ipv6 ospf mtu-ignore
- ipv6 ospf network
- ipv6 ospf priority
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay
- ipv6 router ospf
- maximum-paths
- nsf
- nsf helper
- nsf helper strict-lsa-checking
- nsf restart-interval
- passive-interface
- passive-interface default
- redistribute
- router-id
- show ipv6 ospf
- show ipv6 ospf abr
- show ipv6 ospf area
- show ipv6 ospf asbr
- show ipv6 ospf database
- show ipv6 ospf database database-summary
- show ipv6 ospf interface
- show ipv6 ospf interface brief
- show ipv6 ospf interface stats
- show ipv6 ospf interface vlan
- show ipv6 ospf neighbor
- show ipv6 ospf range
- show ipv6 ospf stub table

- `show ipv6 ospf virtual-link`
- `show ipv6 ospf virtual-link brief`

area default-cost

Use the **area default-cost** command in Router OSPFv3 Configuration mode to configure the monetary default cost for the stub area. The operator must specify the area id and an integer value between 1-16777215. Use the no form of the command to return the cost to the default value.

Syntax

area *areaid* **default-cost** *cost*

no area *areaid* **default-cost**

- *areaid* — Valid area identifier.
- *cost* — Default cost. (Range: 1-16777215)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the monetary default cost at 100 for stub area 1.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 default-cost 100
```

area nssa

Use the **area nssa** command in Router OSPFv3 Configuration mode to configure the specified areaid to function as an NSSA.

Syntax

area *areaid* **nssa**

no area *areaid* **nssa**

- *areaid* — Valid OSPFv3 area identifier.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures area 1 to function as an NSSA.

```
console(config)#ipv6 router ospf
```

```
console(config-rtr)#area 1 nssa
```

area nssa default-info-originate

Use the **area nssa default-info-originate** command in Router OSPFv3 Configuration mode to configure the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route. The metric type can be comparable (**nssa-external 1**) or noncomparable (**nssa-external 2**). Use the **no** form of the command to return the metric value and type to the default value

Syntax

area *areaid* **nssa default-info-originate** [*metric* [**comparable** | **non-comparable**]]

no area *areaid* **nssa default-info-originate**

- *areaid* — Valid OSPFv3 area identifier.
- *metric* — Metric value for default route. (Range: 1-16777214)

- **comparable** — Metric Type (nssa-external 1).
- **non-comparable** — Metric Type (nssa-external 2).

Default Configuration

If no metric is defined, 10 is the default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the default metric value for the default route advertised into the NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa default-info-originate
```

area nssa no-redistribute

Use the **area nssa no-redistribute** command in Router OSPFv3 Configuration mode to configure the NSSA ABR so that learned external routes will not be redistributed to the NSSA. Use the **no** form of the command to remove the configuration.

Syntax

area *areaid* nssa no-redistribute

no area *areaid* nssa no-redistribute

- *areaid* — Valid OSPF area identifier.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the area 1 NSSA ABR so that learned external routes will not be redistributed to the NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa no-redistribute
```

area nssa no-summary

Use the **area nssa no-summary** command in Router OSPFv3 Configuration mode to configure the NSSA so that summary LSAs are not advertised into the NSSA. Use the no form of the command to remove the configuration.

Syntax

area *areaid* **nssa no-summary**

no area *area-id* **nssa no-summary**

- *areaid*— Valid OSPF area identifier.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the area 1 NSSA so that summary LSAs are not advertised into the NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 nssa no-summary
```

area nssa translator-role

Use the **area nssa translator-role** command in Router OSPFv3 Configuration mode to configure the translator role of the NSSA. Use the **no** form of the command to remove the configuration.

Syntax

```
area areaid nssa translator-role {always | candidate}
```

```
no area areaid nssa translator-role
```

- *areaid* — Valid OSPF area identifier.
- **always** — Causes the router to assume the role of the translator the instant it becomes a border router.
- **candidate** — Causes the router to participate in the translator election process when it attains border router status.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the **always** translator role of the area 1 NSSA.

```
console(config)#ipv6 router ospf
```

```
console(config-rtr)#area 1 nssa translator-role  
always
```

area nssa translator-stab-intv

Use the **area nssa translator-stab-intv** command in Router OSPFv3 Configuration mode to configure the translator stability interval of the NSSA. The stability interval is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Syntax

area *areaid* **nssa translator-stab-intv** *seconds*

no area *areaid* **nssa translator-stab-intv**

- *areaid* — Valid OSPF area identifier.
- *seconds* — Translator stability interval of the NSSA. (Range: 0-3600 seconds)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a translator stability interval of 100 seconds for the area 1 NSSA.

```
console(config)#ipv6 router ospf  
console(config-rtr)#area 1 nssa translator-stab-intv  
100
```

area range

Use the **area range** command in Router OSPF Configuration mode to configure a summary prefix for routes learned in a given area. There are two types of area ranges. An area range can be configured to summarize intra-area routes. An ABR advertises the range rather than the specific intra-area route as a type 3 summary LSA. Also, an area range can be configured at the edge of an NSSA to summarize external routes reachable within the NSSA. The range is advertised as a type 5 external LSA. Use the **no** form of the command to remove the summary prefix configuration for routes learned in the specified area.

Syntax

```
area areaid range ipv6-prefix/prefix-length {summarylink | nssaexternallink}
[advertise | not-advertise]
```

```
no area areaid range ipv6-prefix/prefix-length {summarylink |
nssaexternallink}
```

- *areaid* — Valid OSPF area identifier.
- *ipv6-prefix/prefix-length* — Valid route prefix.
- **summarylink** — LSDB type
- **nssaexternallink** — LSDB type.
- **advertise** — Allows area range to be advertised.
- **not-advertise** — Suppresses area range from being advertised.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

The LSDB type must be specified by either **summarylink** or **nssaexternallink**, and the advertising of the area range can be allowed or suppressed.

Example

The following example creates an area range for the area 1 NSSA.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 range 2020:1::1/64
summarylink
```

area stub

Use the **area stub** command in Router OSPFv3 Configuration mode to create a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Syntax

area *areaid* **stub**

no area *areaid* **stub**

- *areaid*— Valid OSPFv3 area identifier.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example creates a stub area for area 1.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 stub
```

area stub no-summary

Use the **area stub no-summary** command in Router OSPFv3 Configuration mode to disable the import of Summary LSAs for the stub area identified by *areaid*.

Syntax

area *areaid* stub no-summary

no area *areaid* stub no-summary

- *areaid* — Valid OSPFv3 area identifier.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example prevents Summary LSAs from being advertised into the area 1 NSSA.

```
console(config)#ipv6 router ospf
```

```
console(config-rtr)#area 1 stub no-summary
```

area virtual-link

Use the **area virtual-link** command in Router OSPFv3 Configuration mode to create the OSPF virtual interface for the specified *areaid* and *neighbor*. Use the **no area virtual-link** command to delete an OSPF virtual interface in an area.

Syntax

area *areaid* virtual-link *neighbor-id*

no area *areaid* virtual-link *neighbor-id*

- *areaid*— Valid OSPFv3 area identifier (or decimal value in the range of 0-4294967295).
- *neighbor-id*— Identifies the Router ID or IP address of the neighbor.

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example creates the OSPF virtual interface for area 1 and its neighbor router.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2
```

area virtual-link dead-interval

Use the **area virtual-link dead-interval** command in Router OSPFv3 Configuration mode to configure the dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Syntax

area *areaid* virtual-link *neighbor* dead-interval *seconds*

no area *areaid* virtual-link *neighbor* dead-interval

- *areaid*— Valid OSPFv3 area identifier.
- *neighbor*— Router ID of neighbor.
- *seconds*— Dead interval. (Range: 1-65535)

Default Configuration

40 is the default value for *seconds*.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a 20-second dead interval for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2 dead-
interval 20
```

area virtual-link hello-interval

Use the **area virtual-link hello-interval** command in Router OSPFv3 Configuration mode to configure the hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Syntax

area *areaid* **virtual-link** *neighbor* **hello-interval** *seconds*

no area *areaid* **virtual-link** *neighbor* **hello-interval**

- *areaid* — Valid OSPFv3 area identifier.
- *neighbor* — Router ID of neighbor.
- *seconds* — Hello interval. (Range: 1-65535)

Default Configuration

10 is the default value for *seconds*.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a hello interval of 20 seconds for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
console(config)#ipv6 router ospf
console(config-rtr)#area 1 virtual-link 2 hello-
interval 20
```

area virtual-link retransmit-interval

Use the **area virtual-link retransmit-interval** command in Router OSPFv3 Configuration mode to configure the retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Syntax

area *areaid* **virtual-link** *neighbor* **retransmit-interval** *seconds*
no area *areaid* **virtual-link** *neighbor* **retransmit-interval**

- *areaid*— Valid OSPFv3 area identifier.
- *neighbor*— Router ID of neighbor.
- *seconds*— Retransmit interval. (Range: 0-3600)

Default Configuration

5 is the default value for *seconds*.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures the retransmit interval of 20 seconds for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
(config)#ipv6 router ospf
(config-rtr)#area 1 virtual-link 2 retransmit-
interval 20
```

area virtual-link transmit-delay

Use the **area virtual-link transmit-delay** command in Router OSPFv3 Configuration mode to configure the transmit delay for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Syntax

area *areaid* **virtual-link** *neighbor* **transmit-delay** *seconds*
no area *areaid* **virtual-link** *neighbor* **transmit-delay**

- *areaid* — Valid OSPFv3 area identifier.
- *neighbor* — Router ID of neighbor.
- *seconds* — Transmit delay interval. (Range: 0-3600)

Default Configuration

1 is the default value for *seconds*.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a 20-second transmit delay for the OSPF virtual interface on the virtual interface identified by area 1 and its neighbor.

```
console(config)#ipv6 router ospf
```

```
console(config-rtr)#area 1 virtual-link 2 transmit-  
delay 20
```

default-information originate

Use the **default-information originate** command in Router OSPFv3 Configuration mode to control the advertisement of default routes. Use the **no** form of the command to return the default route advertisement settings to the default value.

Syntax

default-information originate [**always**] [**metric** *integer*] [**metric-type** {1 | 2}]

no default-information originate [**metric**] [**metric-type**]

- **always** — Always advertise default routes.
- *integer* — The metric (or preference) value of the default route. (Range: 1–16777214)
- 1—External type-1 route.
- 2—External type-2 route.
- **metric** — Specify the metric of the default route.
- **metric-type** — Specify metric-type of the default route.

Default Configuration

2 is the default value for **metric-type**.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example controls the advertisement of default routes by defining a metric value of 100 and metric type 2.

```
console(config)#ipv6 router ospf
```

```
console(config-rtr)#default-information originate  
metric 100 metric-type 2
```

default-metric

Use the **default-metric** command in Router OSPFv3 Configuration mode to set a default for the metric of distributed routes.

Syntax

default-metric *metric*

no default-metric

- *metric* — Metric value used for distribution (Range: 1-16777214)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets a default of 100 for the metric of distributed routes.

```
console(config)#ipv6 router ospf  
console(config-rtr)#default-metric 100
```

distance ospf

The **distance ospf** command sets the preference values of OSPF route types in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, external. All the external type routes are given the same preference value. Use the “no” form of this command to reset the preference values to the default.

Syntax

`distance ospf {external | inter-area | intra-area } distance`

`no distance ospf {external | inter-area | intra-area } distance`

- *distance*— Used to select the best path when there are two or more routes to the same destination from two different routing protocols (Range: 1–255).

Default Configuration

The default preference value is 110.

Command Mode

Router OSPF Configuration mode.

Router OSPFv3 Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example sets a route preference value of 100 for intra OSPF in the router.

```
console(config)#ipv6 router ospf
console(config-rtr)#distance ospf intra 100
```

enable

Use the **enable** command in Router OSPFv3 Configuration mode to enable administrative mode of OSPF in the router (active).

Syntax

`enable`

`no enable`

Default Configuration

Enabled is the default state.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example enables administrative mode of OSPF in the router (active).

```
console(config)#ipv6 router ospf
console(config-rtr)#enable
```

exit-overflow-interval

Use the **exit-overflow-interval** command in Router OSPFv3 Configuration mode to configure the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to originate non-default AS-external-LSAs again. When set to 0, the router will not leave Overflow State until restarted.

Syntax

exit-overflow-interval *seconds*

no exit-overflow-interval

- *seconds* — Exit overflow interval for OSPF (Range: 0-2147483647)

Default Configuration

0 is the default value for *seconds*.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the exit overflow interval for OSPF at 100 seconds.

```
console(config)#ipv6 router ospf
console(config-rtr)#exit-overflow-interval 100
```

external-lsdb-limit

Use the **external-lsdb-limit** command in Router OSPFv3 Configuration mode to configure the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default ASexternal- LSAs in it database. The external LSDB limit **MUST** be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area.

Syntax

external-lsdb-limit *limit*

no external-lsdb-limit

- *limit* — External LSDB limit for OSPF (Range: -1-2147483647)

Default Configuration

-1 is the default value for *limit*.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the external LSDB limit at 100 for OSPF.

```
console(config)#ipv6 router ospf
console(config-rtr)#external-lsdb-limit 100
```

ipv6 ospf

Use the **ipv6 ospf** command in Interface Configuration mode to enable OSPF on a router interface or loopback interface.

Syntax

```
ipv6 ospf
no ipv6 ospf
```

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables OSPF on VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf
```

ipv6 ospf areaid

Use the **ipv6 ospf areaid** command in Interface Configuration mode to set the OSPF area to which the specified router interface belongs.

Syntax

ipv6 ospf areaid *areaid*

no ipv6 ospf areaid *areaid*

- *areaid* — Is a 32-bit integer, formatted as a 4-digit dotted-decimal number or a decimal value. It uniquely identifies the area to which the interface connects. Assigning an area id which does not exist on an interface causes the area to be created with default values. (Range: 0-4294967295).

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example defines the OSPF area to which VLAN 15 belongs.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ipv6 ospf areaid 100
```

ipv6 ospf cost

Use the **ipv6 ospf cost** command in Interface Configuration mode to configure the cost on an OSPF interface.

Syntax

ipv6 ospf cost *cost*

no ipv6 ospf cost

- *cost* — Cost for OSPF interface. (Range: 1-65535)

Default Configuration

10 is the default value of *cost*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a cost of 100.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf cost 100
```

ipv6 ospf dead-interval

Use the **ipv6 ospf dead-interval** command in Interface Configuration mode to set the OSPF dead interval for the specified interface.

Syntax

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval

- *seconds* — A valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). (Range: 1-65535)

Default Configuration

40 seconds is the default value of *seconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF dead interval at 100 seconds.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf dead-interval 100
```

ipv6 ospf hello-interval

Use the **ipv6 ospf hello-interval** command in Interface Configuration mode to set the OSPF hello interval for the specified interface.

Syntax

ipv6 ospf hello-interval *seconds*

no ipv6 ospf hello-interval

- *seconds* — A valid positive integer which represents the length of time of the OSPF hello interval. The value must be the same for all routers attached to a network. (Range: 1-65535 seconds)

Default Configuration

10 seconds is the default value of *seconds*.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF hello interval at 15 seconds.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf hello-interval 15
```

ipv6 ospf mtu-ignore

Use the **ipv6 ospf mtu-ignore** command in Interface Configuration mode to disable OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Syntax

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Default Configuration

Enabled is the default state.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example disables OSPF maximum transmission unit (MTU) mismatch detection.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ipv6 ospf mtu-ignore
```

ipv6 ospf network

Use the **ipv6 ospf network** command in Interface Configuration mode to change the default OSPF network type for the interface. Normally, the network type is determined from the physical IP network type. By default all Ethernet networks are OSPF-type broadcast. Similarly, tunnel interfaces

default to point-to-point. When an Ethernet port is used as a single large bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers. Using point-to-point as the network type eliminates the overhead of the OSPF designated router election. It is normally not useful to set a tunnel to OSPF network type broadcast.

Syntax

```
ipv6 ospf network { broadcast | point-to-point }
```

```
no ipv6 ospf network
```

- **broadcast** — The network type is broadcast.
- **point-to-point** — The network type is point-to-point.

Default Configuration

Broadcast is the default state.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode

User Guidelines

This command has no user guidelines.

Example

The following example changes the default OSPF network type to point-to-point.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ipv6 ospf network point-to-point
```

ipv6 ospf priority

Use the **ipv6 ospf priority** command in Interface Configuration mode to set the OSPF priority for the specified router interface.

Syntax

`ipv6 ospf priority priority`

`no ipv6 ospf priority`

- *priority* — OSPF priority for specified interface. (Range: 0-255. A value of 0 indicates that the router is not eligible to become the designated router on this network)

Default Configuration

1, the highest router priority, is the default value.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF priority at 50 for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ipv6 ospf priority 50
```

ipv6 ospf retransmit-interval

Use the `ipv6 ospf retransmit-interval` command in Interface Configuration mode to set the OSPF retransmit interval for the specified interface.

Syntax

`ipv6 ospf retransmit-interval seconds`

`no ipv6 ospf retransmit-interval`

- *seconds* — The number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. (Range: 0 to 3600 seconds)

Default Configuration

5 seconds is the default value.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF retransmit interval at 100 seconds.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf retransmit-
interval 100
```

ipv6 ospf transmit-delay

Use the **ipv6 ospf transmit-delay** command in Interface Configuration mode to set the OSPF Transmit Delay for the specified interface.

Syntax

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay

- *seconds* — OSPF transmit delay for the specified interface. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. (Range: 1 to 3600 seconds)

Default Configuration

No default value.

Command Mode

Interface Configuration (VLAN, Tunnel, Loopback) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the OSPF Transmit Delay at 100 seconds for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ipv6 ospf transmit-delay
100
```

ipv6 router ospf

Use the **ipv6 router ospf** command in Global Configuration mode to enter Router OSPFv3 Configuration mode.

Syntax

ipv6 router ospf

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

Use the following command to enable OSPFv3.

```
console(config)#ipv6 router ospf
```

maximum-paths

Use the **maximum-paths** command in Router OSPFv3 Configuration mode to set the number of paths that OSPF can report for a given destination.

Syntax

`maximum-paths` *maxpaths*

`no maximum-paths`

- *maxpaths* — Number of paths that can be reported. (Range: 1-2)

Default Configuration

2 is the default value for *maxpaths*.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the number of paths that OSPF can report for a destination to 1.

```
console(config)#ipv6 router ospf
console(config-rtr)#maximum-paths 1
```

nsf

Use this command to enable OSPF graceful restart. Use the “no” form of this command to disable graceful restart.

Syntax

`nsf` [*ietf*] [*planned-only*]

`no nsf` [*ietf*]

ietf — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.

planned-only — This keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).

Default Configuration

Graceful restart is disabled by default

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

Graceful restart works in concert with nonstop forwarding to enable the hardware to continue forwarding IPv6 packets using OSPFv3 routes while a backup unit takes over management unit responsibility. When OSPF executes a graceful restart, it informs its neighbors that the OSPF control plane is restarting, but that it will be back shortly. Helpful neighbors continue to advertise to the rest of the network that they have full adjacencies with the restarting router, avoiding announcement of a topology change and everything that goes with that (i.e., flooding of LSAs, SPF runs). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

This implementation of graceful restart restarting router behavior is only useful with a router stack. Graceful restart does not work on a standalone, single-unit router.

Example

—

nsf helper

Use the **nsf-helper** to allow OSPF to act as a helpful neighbor for a restarting router. Use the “no” form of this command to prevent OSPF from acting as a helpful neighbor.

Syntax

nsf helper[planned-only]

no nsf helper

- **planned-only** — This keyword indicates that OSPF should only help a restarting router performing a planned restart.

Default Configuration

OSPF may act as a helpful neighbor for both planned and unplanned restarts

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

The grace LSA announcing the graceful restart includes a restart reason. Reasons 1 (software restart) and 2 (software reload/upgrade) are considered planned restarts. Reasons 0 (unknown) and 3 (switch to redundant control processor) are considered unplanned restarts.

nsf ietf helper disable is functionally equivalent to no nsf helper and is supported solely for IS CLI compatibility.

Example

—

nsf helper strict-lsa-checking

Use the **nsf-helper strict-lsa-checking** command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs. Use the “no” form of this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Syntax

nsf [ietf] helper strict-lsa-checking

no nsf [ietf] helper strict-lsa-checking

- **ietf** —This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.

Default Configuration

A helpful neighbor exits helper mode when a topology change occurs.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router.

A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Example

—

nsf restart-interval

Use the **nsf restart-interval** command to configure the length of the grace period on the restarting router. Use the “no” form of this command to revert the grace period to its default.

Syntax

nsf [**ietf**] **restart-interval** *seconds*

no nsf [**ietf**] **restart-interval**

- **ietf** — This keyword is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is the only one supported, this keyword is optional.
- *seconds* — The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The restarting router includes the restart interval in its grace LSAs (range 1–1800 seconds).

Default Configuration

The default restart interval is 120 seconds.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Example

—

passive-interface

Use the **passive-interface** command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel. Use the “no” form of this command to set the interface or tunnel as non-passive.

Syntax

passive-interface {vlan *vlan-id* | tunnel *tunnel-id*}

no passive-interface {vlan *vlan-id* | tunnel *tunnel-id*}

- *vlan-id* — The vlan number
- *tunnel-id* — Tunnel identifier. (Range: 0–7)

Default Configuration

Passive interface mode is disabled by default.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-router)#passive-interface vlan 1
```

passive-interface default

The **passive-interface default** command enables the global passive mode by default for all interfaces. It overrides any interface level passive mode. Use the “no” form of this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Syntax

passive-interface default

no passive-interface default

Default Configuration

Global passive mode is disabled by default.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-rtr)#passive-interface default
```

redistribute

Use the **redistribute** command in Router OSPFv3 Configuration mode to configure the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

Syntax

redistribute {static | connected} [metric *metric*] [metric-type {1 | 2}] [**tag** *tag*]

no redistribute {static | connected} [*metric*] [metric-type] [*tag*]

- *metric* — Metric value used for default routes. (Range: 0-16777214)
- *tag* — Tag. (Range: 0-4294967295)

Default Configuration

2 is the default value for **metric-type**, 0 for *tag*.

Command Mode

Router OSPFv3 Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

```
console(config)#ipv6 router ospf
```

```
console(config-rtr)#redistribute connected
```

router-id

Use the **router-id** command in Router OSPFv3 Configuration mode to set a 4-digit dotted-decimal number uniquely identifying the Router OSPF ID.

Syntax

router-id *router-id*

- *router-id* — Router OSPF identifier. (Range: 0-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Router OSPFv3 Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets a 4-digit dotted-decimal number identifying the Router OSPF ID as 2.3.4.5.

```
console(config)#ipv6 router ospf
console(config-rtr)#router-id 2.3.4.5
```

show ipv6 ospf

Use the `show ipv6 ospf` command in Privileged EXEC mode to display information relevant to the OSPF router.

Syntax

```
show ipv6 ospf
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

Some of the information below displays only if you enable OSPF and configure certain features. The following fields may be displayed:

Router ID	A 32-bit integer in dotted decimal format identifying the router about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether OSPF is administratively enabled or disabled.

External LSDB Limit	Shows the maximum number of non-default external LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	Shows the number of seconds that, after entering OverflowState, as defined by RFC 1765, a router will attempt to leave OverflowState.
AutoCost Ref BW	The configured autcost reference bandwidth. This value is used to determine the OSPF metric on its interfaces. The reference bandwidth is divided by the interface speed to compute the metric.
Default Passive Setting	When enabled, OSPF interfaces are passive by default.
Maximum Paths	Shows the maximum number of paths that OSPF can report for a given destination.
Default Metric	Default metric for redistributed routes.
Default Route Advertise	When enabled, OSPF originates a type 5 LSA advertising a default route.
Always	When this option is configured, OSPF only originates a default route when the router has learned a default route from another source.
Metric	Shows the metric for the advertised default routes. If the metric is not configured, this field is not configured.
Metric Type	Shows whether the metric for the default route is advertised as External Type 1 or External Type 2.
Number of Active Areas	The number of OSPF areas to which the router is attached on interfaces that are up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	Indicates whether the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learned from another protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learned by other protocols) or disabled (if the router is not configured for the same).

Stub Router	OSPF enters stub router mode, as described in RFC 3137, when it encounters a resource limitation that prevents it from computing a complete routing table. In this state, OSPF sets the link metrics of non-stub links in its own router LSAs to the largest possible value, discouraging other routers from computing paths through the stub router, but allowing other routers to compute routes to destinations attached to the stub router. To restore OSPF to normal operation, resolve the condition that caused the resource overload, then disable and re-enable OSPF globally.
External LSDB Overflow	OSPF enters this state when the number of external LSAs exceeds a configured limit, as described in RFC 1765.
External LSA Count	Shows the number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.
New LSAs Originated	Shows the number of link-state advertisements that have been originated.
LSAs Received	Shows the number of link-state advertisements received determined to be new instantiations.
LSA Count	The number of LSAs in the link state database.
Maximum Number of LSAs	The limit on the number of LSAs that the router can store in its link state database.
LSA High Water Mark	The maximum number of LSAs that have been in the link state database since OSPF began operation.
Retransmit List Entries	The current number of entries on all neighbors' retransmit lists.
Maximum Number of Retransmit Entries	The maximum number of entries that can be on neighbors' retransmit lists at any given time. This is the sum for all neighbors. When OSPF receives an LSA and cannot allocate a new retransmit list entry, the router does not acknowledge the LSA, expecting the sender to retransmit.
Retransmit Entries High Water Mark	The maximum number of retransmit list entries that have been on all neighbors' retransmit lists at one time.
NSF Support	Whether graceful restart is administratively enabled. Possible values are Support Always, Disabled, or Planned.

NSF Restart Interval	The number of seconds a helpful neighbor allows a restarting router to complete its graceful restart.
NSF Restart Status	Whether the router is currently performing a graceful restart.
NSF Restart Age	The number of seconds until a graceful restart expires. Only non-zero when the router is in graceful restart.
NSF Restart Exit Reason	The reason the previous graceful restart ended. Possible values are Not attempted, In progress, Completed, Timed out, Topology change, and Manual clear.
NSF Helper Support	Whether this router is configured to act as a graceful restart helpful neighbor. Possible values are: Helper Support Always, Disabled, or Planned.
NSF Helper Strict LSA Checking	As a graceful restart helpful neighbor, whether to terminate the helper relationship if a topology change occurs during a neighbor's graceful restart.
Redistributing	This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.
Source	Shows source protocol/routes that are being redistributed. Possible values are static, connected, or RIP.
Tag	Shows the decimal value attached to each external route.
Subnets	When this option is not configured, OSPF will only redistribute classful prefixes.
Distribute-List	Shows the access list used to filter redistributed routes.

Example

The following example enables OSPF traps.

```

console#show ipv6 ospf
Router ID..... 0.0.0.2
OSPF Admin Mode..... Enable
ASBR Mode..... Disable
ABR Status..... Disable
Exit Overflow Interval..... 0
External LSA Count..... 0
External LSA Checksum..... 0

```

```

New LSAs Originated..... 0
LSAs Received..... 0
External LSDB Limit..... No Limit
Default Metric..... Not Configured
Maximum Paths..... 2
Default Route Advertise..... Disabled
Always..... FALSE
Metric.....
Metric Type..... External Type 2
NSF Support..... Disabled
NSF Restart Interval..... 120 seconds
NSF Helper Support..... Always
NSF Helper Strict LSA Checking..... Enabled

```

show ipv6 ospf abr

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR). This command takes no options.

Syntax

```
show ipv6 ospf abr
```

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode.

User Guidelines

This command has no user guidelines.

Example

```
console#show ipv6 ospf abr
```

Type	Router Id	Cost	Area ID	Next Hop	Next Hop Intf
INTRA	3.3.3.3	10	0.0.0.1	FE80::211:88FF:FE2A:3CB3	vlan11
INTRA	4.4.4.4	10	0.0.0.1	FE80::210:18FF:FE82:8E1	vlan12

show ipv6 ospf area

Use the `show ipv6 ospf area` command in Privileged EXEC mode to display information about the area.

Syntax

```
show ipv6 ospf area areaid
```

- areaid*— Identifier for the OSPF area being displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays information about area 1.

```
console#show ipv6 ospf area 1
```

AreaID.....	0.0.0.1
External Routing.....	Import External LSAs
Spf Runs.....	0
Area Border Router Count.....	0

```
Area LSA Count..... 0
Area LSA Checksum..... 0
Stub Mode..... Disable
Import Summary LSAs..... Enable
```

show ipv6 ospf asbr

The `show ipv6 ospf asbr` command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routes (ASBR). This command takes no options.

Syntax

`show ipv6 ospf asbr`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

```
console#show ipv6 ospf asbr
```

Type	Router Id	Cost	Area ID	Next Hop	Next Hop Intf
----	-----	----	-----	-----	-----
INTRA	1.1.1.1	10	0.0.0.1	FE80::213:C4FF:FEDB:6C41	vlan10
INTRA	4.4.4.4	10	0.0.0.1	FE80::210:18FF:FE82:8E1	vlan12

show ipv6 ospf database

Use the **show ipv6 ospf database** command in Privileged EXEC mode to display information about the link state database when OSPFv3 is enabled. If no parameters are entered, the command displays the LSA headers. Optional parameters specify the type of link state advertisements to display.

The information below is only displayed if OSPF is enabled.

Syntax

```
show ipv6 ospf [areaid] database [{external | inter-area {prefix | router} |  
link | network | nssa-external | prefix | router | unknown [area | as |  
link]}] [lsid] [adv-router [rtrid] | self-originate]
```

- *areaid*— Identifies a specific OSPF area for which link state database information will be displayed.
- **external** — Displays the external LSAs.
- **inter-area** — Displays the inter-area LSAs.
- **link** — Displays the link LSAs.
- **network** — Displays the network LSAs.
- **nssa-external** — Displays NSSA external LSAs.
- **prefix** — Displays intra-area Prefix LSA.
- **router** — Displays router LSAs.
- **unknown** — Displays unknown area, AS or link-scope LSAs.
- *lsid*— Specifies a valid link state identifier (LSID).
- **adv-router** — Shows the LSAs that are restricted by the advertising router.
- *rtrid*— Specifies a valid router identifier.
- **self-originate** — Displays the LSAs in that are self originated.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the link state database when OSPFv3 is enabled.

```
console#show ipv6 ospf database

                        Router Link States (Area 0.0.0.0)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
1.1.1.1          0      4      80000034 54BD V6E--R- ----B
2.2.2.2          0      2      80000044 95A5 V6E--R- ----B

                        Network Link States (Area 0.0.0.0)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
2.2.2.2          636     636     80000001 8B0D V6E--R-

                        Inter Network States (Area 0.0.0.0)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
1.1.1.1          1      323     80000001 3970
2.2.2.2          1      322     80000001 1B8A
1.1.1.1          2      293     80000001 3529
2.2.2.2          2      375     80000001 FC5E

                        Link States (Area 0.0.0.0)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
1.1.1.1          634     700     80000008 2D89 V6E--R-
2.2.2.2          634     689     8000000A 6F82 V6E--R-
2.2.2.2          635     590     80000001 7782 V6E--R-
```

```

Intra Prefix States (Area 0.0.0.0)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
1.1.1.1         0      1      8000003C 9F31
2.2.2.2         0      2      8000004D 9126

```

```

Router Link States (Area 0.0.0.1)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
1.1.1.1         0      1      8000002E 35AD V6E--R- --V-B
2.2.2.2         0      0      8000004A D2F3 V6E--R- ----B

```

```

Network Link States (Area 0.0.0.1)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
1.1.1.1         634    621    80000001 B9E2 V6E--R-

```

```

Inter Network States (Area 0.0.0.1)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
1.1.1.1         16      4      80000001 CA7C
2.2.2.2         18      3      80000001 B28D

```

```

Link States (Area 0.0.0.1)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
1.1.1.1         634    441    80000003 B877 V6E--R-
2.2.2.2         634    433    80000003 FE6E V6E--R-

```

```

Intra Prefix States (Area 0.0.0.1)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt

```

-----	-----	-----	-----
1.1.1.1	0	6	8000003A 37C4
2.2.2.2	0	1	8000004F 439A
1.1.1.1	10634	434	80000002 440A

show ipv6 ospf database database-summary

Use the `show ipv6 ospf database database-summary` command in Privileged EXEC mode to display the number of each type of LSA in the database and the total number of LSAs in the database.

Syntax

`show ipv6 ospf database database-summary`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the number of each type of LSA in the database and the total number of LSAs in the database.

```
console#show ipv6 ospf database database-summary
OSPF Router with ID (0.0.0.2)
Router database summary
Router..... 0
Network..... 0
Inter-area Prefix..... 0
Inter-area Router..... 0
```

Type-7 Ext.....	0
Link.....	0
Intra-area Prefix.....	0
Link Unknown.....	0
Area Unknown.....	0
AS Unknown.....	0
Type-5 Ext.....	0
Self-Originated Type-5 Ext.....	0
Total.....	0

show ipv6 ospf interface

Use the `show ipv6 ospf interface` command in Privileged EXEC mode to display the information for the IFO object or virtual interface tables.

Syntax

`show ipv6 ospf interface {vlan vlan-id| tunnel tunnel-id | loopback loopback-id}`

- *vlan-id*— Valid VLAN ID.
- *tunnel-id*— Tunnel identifier. (Range: 0-7)
- *loopback-id*— Loopback identifier. (Range: 0-7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the information in VLAN 11's virtual interface tables.

```
console#show ipv6 ospf interface vlan 11
IP Address..... Err
ifIndex..... 1
OSPF Admin Mode..... Enable
OSPF Area ID..... 0.0.0.0
Router Priority..... 1
Retransmit Interval..... 5
Hello Interval..... 10
Dead Interval..... 40
LSA Ack Interval..... 1
Iftransit Delay Interval..... 1
Authentication Type..... None
Metric Cost..... 10 (computed)
OSPF Mtu-ignore..... Disable
OSPF cannot be initialized on this interface.
```

show ipv6 ospf interface brief

Use the `show ipv6 ospf interface brief` command in Privileged EXEC mode to display brief information for the IFO object or virtual interface tables.

Syntax

```
show ipv6 ospf interface brief
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays brief ospf interface information.

```
console#show ipv6 ospf interface brief
```

	Admin		Router		Int.	Int.	Int.	Retrax	LSA
Interface	Mode	Area ID	Prior.	Cost	Val.	Val.	Val.	Delay	Ack
Intval									

show ipv6 ospf interface stats

Use the `show ipv6 ospf interface stats` command in User EXEC mode to display the statistics for a specific interface. The command only displays information if OSPF is enabled.

Syntax

```
show ipv6 ospf interface stats vlan vlan-id
```

- *vlan-id* — Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the interface statistics for VLAN 5.

```
console>show ipv6 ospf interface stats vlan 5
OSPFv3 Area ID..... 0.0.0.1
Spf Runs..... 265
Area Border Router Count..... 1
AS Border Router Count..... 0
Area LSA Count..... 6
IPv6 Address.....
FE80::202:BCFF:FE00:3146/1283FFE::2/64
OSPF Interface Events..... 53
Virtual Events..... 13
Neighbor Events..... 6
External LSA Count..... 0
LSAs Received..... 660
Originate New LSAs..... 853
Sent Packets..... 1013
Received Packets..... 893
Discards..... 48
Bad Version..... 0
Virtual Link Not Found..... 9
Area Mismatch..... 39
Invalid Destination Address..... 0
No Neighbor at Source Address..... 0
Invalid OSPF Packet Type..... 0
    Packet Type          Sent          Received
-----
Hello                    295          219
Database Description     10           14
```


LS Request	4	4
LS Update	521	398
LS Acknowledgement	209	282

show ipv6 ospf interface vlan

Use the `show ipv6 ospf interface vlan` command in Privileged EXEC mode to display OSPFv3 configuration and status information for a specific vlan.

Syntax

`show ipv6 ospf interface vlan { vlan-id | brief }`

- *vlan-id* — Valid VLAN ID. Range is 1-4093.
- **brief** — Displays a snapshot of configured interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays ospf interface vlan information.

```
console#show ipv6 ospf interface vlan 10
IPv6 Address.....
FE80::2FC:E3FF:FE90:44
ifIndex..... 634
OSPF Admin Mode..... Enable
OSPF Area ID..... 0.0.0.1
Router Priority..... 1
Retransmit Interval..... 5
```

```

Hello Interval..... 10
Dead Interval..... 40
LSA Ack Interval..... 1
Iftransit Delay Interval..... 1
Authentication Type..... None
Metric Cost..... 10 (computed)
OSPF Mtu-ignore..... Disable
OSPF Interface Type..... broadcast
State..... backup-
designated-router
Designated Router..... 1.1.1.1
Backup Designated Router..... 2.2.2.2
Number of Link Events..... 46

```

show ipv6 ospf neighbor

Use the **show ipv6 ospf neighbor** command in Privileged EXEC mode to display information about OSPF neighbors. If a neighbor IP address is not specified, the output displays summary information in a table. If an interface or tunnel is specified, only the information for that interface or tunnel displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Syntax

```
show ipv6 ospf neighbor [ interface { vlan vlan-id | tunnel tunnel-id } ] [ ip-
address ]
```

- *vlan-id* — Valid VLAN ID.
- *tunnel-id* — Tunnel identifier. (Range: 0-7)
- *ip-address* — Is the valid IP address of the neighbor about which information is displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Examples

The following examples display information about OSPF neighbors, in the first case in a summary table, and in the second in a table specific to tunnel 1.

```
console#show ipv6 ospf neighbor
```

Router ID	Priority	Intf	Interface	State	Dead
		ID			Time
-----	-----	-----	-----	-----	----

```
console#show ipv6 ospf neighbor interface tunnel 1
```

```
IP Address..... Err
ifIndex..... 619
OSPF Admin Mode..... Enable
OSPF Area ID..... 0.0.0.0
Router Priority..... 1
Retransmit Interval..... 5
Hello Interval..... 10
Dead Interval..... 40
LSA Ack Interval..... 1
Iftransit Delay Interval..... 1
Authentication Type..... None
Metric Cost..... 1
(computed)
OSPF Mtu-ignore..... Disable
OSPF cannot be initialized on this interface.
```

show ipv6 ospf range

Use the `show ipv6 ospf range` command in Privileged EXEC mode to display information about the area ranges for the specified area identifier.

Syntax

`show ipv6 ospf range areaid`

- *areaid* — Identifies the OSPF area whose ranges are being displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the area ranges for area 1.

```
console#show ipv6 ospf range 1
```

Area ID	IPv6 Prefix/Prefix Length	Lsdb Type	Advertisement
-----	-----	-----	-----

show ipv6 ospf stub table

Use the `show ipv6 ospf stub table` command in Privileged EXEC mode to display the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Syntax

`show ipv6 ospf stub table`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF stub table.

```
console#show ipv6 ospf stub table
AreaId          TypeofService  Metric Val    Import SummaryLSA
-----
0.0.0.10        Normal         1             Enable
```

show ipv6 ospf virtual-link

Use the **show ipv6 ospf virtual-link** command in Privileged EXEC mode to display the OSPF Virtual Interface information for a specific area and neighbor.

Syntax

show ipv6 ospf virtual-link *areaid neighbor*

- *areaid*— Identifies the OSPF area whose virtual interface information is being displayed.
- *neighbor*— Router ID of neighbor.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF Virtual Interface information for area 1 and its neighbor.

```
console#show ipv6 ospf virtual-link 1 1.1.1.1
Area ID..... 1
Neighbor Router ID..... 1.1.1.1
Hello Interval..... 10
Dead Interval..... 40
Iftransit Delay Interval..... 1
Retransmit Interval..... 5
State..... point-to-point
Metric..... 10
Neighbor State..... Full
```

show ipv6 ospf virtual-link brief

Use the `show ipv6 ospf virtual-link brief` command in Privileged EXEC mode to display the OSPFV3 Virtual Interface information for all areas in the system.

Syntax

```
show ipv6 ospf virtual-link brief
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the OSPF stub table.

```
console(config)#show ipv6 ospf virtual-link brief
```

Area ID	Neighbor	Hello Interval	Dead Interval	Retransmit Interval	Transit Delay
-----	-----	-----	-----	-----	-----

PIM-DM Commands

This chapter explains the following commands:

- `ip pimdm`
- `show ip pimdm`
- `show ip pimdm interface`
- `show ip pimdm neighbor`

ip pimdm

Use the **ip pimdm** command in Global Configuration mode to enable the administrative mode of PIM-DM in the router.

Syntax

ip pimdm

no ip pimdm

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables PIM-DM in the router.

```
console(config)#ip pimdm
```

show ip pimdm

Use the **show ip pimdm** command in Privileged EXEC mode to display system-wide information for PIM-DM.

Syntax

show ip pimdm

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays system-wide information for PIM-DM.

```
console(config)#show ip pimdm
```

```
Admin Mode..... Disable
```

```
      PIM-DM INTERFACE STATUS
```

```
Interface Interface Mode  Protocol State
```

```
-----
```

show ip pimdm interface

Use the **show ip pimdm interface** command in Privileged EXEC mode to display interface information for PIM-DM on the specified interface.

Syntax

```
show ip pimdm interface vlan vlan-id
```

- *vlan-id* — A valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays interface information for VLAN 11 PIM-DM.

```
console(config)#show ip pimdm interface vlan 11
```

Interface Mode.....
Disable
Hello Interval (secs)..... 30

show ip pimdm neighbor

Use the **show ip pimdm neighbor** command in Privileged EXEC mode to display the neighbor information for PIM-DM on the specified interface.

Syntax

show ip pimdm neighbor [**interface** *vlan* *vlan-id* | **all**]

- *vlan-id*— A valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example display the neighbor information for PIM-DM on all interfaces.

```
console(config)#show ip pimdm neighbor all
```

		Up Time	Expiry Time
Neighbor Addr	Interface	hh:mm:ss	hh:mm:ss

PIM-SM Commands

This chapter explains the following commands:

- ip pimsm
- ip pimsm spt-threshold
- ip pim-trapflags
- show ip pimsm
- show ip pimsm interface
- show ip pimsm neighbor
- show ip pimsm rphash

ip pimsm

Use the **ip pimsm** command in Global Configuration mode to set administrative mode of PIM-SM multicast routing across the router to enabled. IGMP must be enabled before PIM-SM can be enabled.

Syntax

```
ip pimsm  
no ip pimsm
```

Default Configuration

PIM-SM is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables PIM-SM on the router.

```
console(config)#ip pimsm
```

ip pimsm spt-threshold

Use the **ip pimsm spt-threshold** command in Global Configuration mode to configure the Data Threshold rate for the last-hop (or leaf) router to switch to the shortest path. The rate is specified in kilobits per second.

Syntax

```
ip pimsm spt-threshold threshold  
no ip pimsm spt-threshold
```

- *threshold*— Threshold rate. (Range: 0-2000 kilobits/sec)

Default Configuration

50 kilobits/sec is the default rate.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example configures a threshold rate of 100 kilobits/sec.

```
console(config)#ip pimsm spt-threshold 100
```

ip pim-trapflags

Use the **ip pim-trapflags** command in Global Configuration mode to enable the PIM trap mode for both Sparse Mode (SM) and Dense Mode (DM).

Syntax

```
ip pim-trapflags  
no ip pim-trapflags
```

Default Configuration

Disabled is the default state.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example enables PIM trap mode.

```
console(config)#ip pim-trapflags
```

show ip pimsm

Use the `show ip pimsm` command in Privileged EXEC mode to display the system-wide information for PIM-SM.

Syntax

`show ip pimsm`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the system-wide information for PIM-SM.

```
console#show ip pimsm
Admin Mode..... Disable
Join/Prune Interval (secs)..... 60
Data Threshold Rate (Kbps)..... 50
Register Threshold Rate (Kbps)..... 50

      PIM-SM INTERFACE STATUS

Interface  Interface Mode  Protocol State
-----  -

```

show ip pimsm interface

Use the `show ip pimsm interface` command in Privileged EXEC mode to display interface information for PIM-SM on the specified interface.

Syntax

`show ip pimsm interface [vlan vlan-id]`

- *vlan-id* — Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays interface information for VLAN 11 PIM-SM.

```
console#show ip pimsm interface vlan 11
Interface..... 11
IP Address..... 0.0.0.0
Subnet Mask..... 0.0.0.0
Mode..... Disable
Hello Interval (secs)..... 30 secs
CBSR Preference..... 0
CRP Preference..... 0
CBSR Hash Mask Length..... 30
```

show ip pimsm neighbor

Use the `show ip pimsm neighbor` command in Privileged EXEC mode to display neighbor information for PIM-SM on the specified interface.

Syntax

`show ip pimsm neighbor [interface vlan vlan-id | all]`

- *vlan-id* — Valid VLAN ID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays neighbor information for PIM-SM on all interfaces.

```
console#show ip pimsm neighbor all
```

NEIGHBOR TABLE

Interface	IP Address	Up Time	Expiry Time
		(hh:mm:ss)	(hh:mm:ss)

show ip pimsm rphash

Use the **show ip pimsm rphash** command in Privileged EXEC mode to display the RP router being selected from the set of active RP routers. The RP router for the group is selected by using a hash algorithm.

Syntax

```
show ip pimsm rphash groupaddr
```

- *groupaddr* — Valid group IP address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays the RP router being selected from the set of active RP routers.

```
console#show ip pimsm rphash 224.5.5.5
```

There are no static RPs for that group on the router.

Router Discovery Protocol

Commands

Routers can be configured to periodically send router discovery messages to announce their presence to locally attached hosts. The router discovery message advertises one or more IP addresses on the router that hosts can use as their default gateway. Hosts can send a router solicitation message asking any router that receives the message to immediately send a router advertisement, so that the host does not have to wait for the next periodic message.

Router discovery enables hosts to select from among multiple default gateways and switch to a different default gateway if an initially designated gateway goes down.

This chapter explains the following commands:

- `ip irdp`
- `ip irdp address`
- `ip irdp holdtime`
- `ip irdp maxadvertinterval`
- `ip irdp minadvertinterval`
- `ip irdp multicast`
- `ip irdp preference`
- `show ip irdp`

ip irdp

Use the **ip irdp** command in Interface Configuration mode to enable Router Discovery on an interface. Use the no form of the command to disable Router Discovery.

Syntax

ip irdp

no ip irdp

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command has no user guidelines.

Example

The following example enables router discovery on the selected interface.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip irdp
```

ip irdp address

Use the **ip irdp address** command in Interface Configuration mode to configure the address that the interface uses to send the router discovery advertisements. Use the no form of the command to return the address to the default.

Syntax

ip irdp address *ip-address*

no ip irdp address

- *ip-address* — IP address for router discovery advertisements. (Range: 224.0.0.1 [all-hosts IP multicast address] or 255.255.255.255 [limited broadcast address])

Default Configuration

IP address 224.0.0.1 is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines. This command is deprecated in favor of the **ip irdp multicast** command. If you issue this command, the configuration will show the **ip irdp multicast** command instead.

Example

The following example sets the limited broadcast address as the IP address for router discovery advertisements.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp address
255.255.255.255
```

ip irdp holdtime

Use the **ip irdp holdtime** command in Interface Configuration mode to configure the value, in seconds, of the holdtime field of the router advertisement sent from this interface. Use the no form of the command to set the time to the default value.

Syntax

```
ip irdp holdtime integer
no ip irdp holdtime
```

- *integer* — Integer value in seconds of the the holdtime field of the router advertisement sent from this interface. The holdtime must be no less than the maximum advertisement interval and cannot be greater than 9000 seconds.

Default Configuration

The holdtime defaults to 3 times the maximum advertisement interval.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

The holdtime is the length of time that a host considers the router advertisement valid. After the holdtime expires, a host will no longer use the router as its default gateway.

Example

The following example sets hold time at 2000 seconds for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip irdp holdtime 2000
```

ip irdp maxadvertinterval

Use the **ip irdp maxadvertinterval** command in Interface Configuration mode to configure the maximum time, in seconds, allowed between sending router advertisements from the interface. Use the **no** form of the command to set the time to the default value.

Syntax

ip irdp maxadvertinterval *integer*

no ip irdp maxadvertinterval

- *integer* — Maximum time in seconds allowed between sending router advertisements from the interface. (Range: 4 or the minimum advertisement interval, whichever is greater, and 1800 seconds)

Default Configuration

600 seconds is the default value.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

The default values of the minimum advertisement interval and the holdtime depend on the value of the maximum advertisement interval. Setting the maximum advertisement interval changes the minimum advertisement interval and holdtime if those values are at their defaults; so, the maximum advertisement interval should always be set first. If the minimum advertisement interval has been configured to a non-default value, the maximum advertisement interval cannot be configured to a lower value than the minimum advertisement interval. If the holdtime has been configured to a non-default value, the maximum advertisement interval cannot be configured to a value larger than the holdtime.

Example

The following example sets maximum advertisement interval at 600 seconds for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp maxadvertinterval
600
```

ip irdp minadvertinterval

Use the **ip irdp minadvertinterval** command in Interface Configuration mode to configure the minimum time, in seconds, allowed between sending router advertisements from the interface. Use the **no** form of the command to set the time to the default value.

Syntax

```
ip irdp minadvertinterval integer
no ip irdp minadvertinterval
```

- *integer* — Minimum time in seconds allowed between sending router advertisements from the interface. (Range: 3 to value of maximum advertisement interval in seconds)

Default Configuration

The default value is 0.75 times the maximum advertisement interval.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets minimum advertisement interval at 100 seconds for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip irdp minadvertinterval
100
```

ip irdp multicast

To send router advertisements as IP multicast packets, use the **ip irdp multicast** command in Interface Configuration mode. To send router advertisements to the limited broadcast address (255.255.255.255), use the **no** form of this command.

Syntax

ip irdp multicast

no ip irdp multicast

Default Configuration

Router discovery packets are sent to the all hosts IP multicast address (224.0.0.1) by default.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

If a subnet includes any hosts that do not accept IP multicast packets, send router advertisements to the limited broadcast address.

Example

The following example configures router discovery to send to the limited broadcast address:

```
console(config)#interface vlan 15804
(config-if-vlan15)#no ip irdp multicast
```

ip irdp preference

Use the **ip irdp preference** command in Interface Configuration mode to configure the preference of the address as a default router address relative to other router addresses on the same subnet. Use the **no** form of the command to set the preference to the default value.

Syntax

ip irdp preference *integer*

no ip irdp preference

- *integer* — Preference of the address as a default router address, relative to other router addresses on the same subnet. (Range: -2147483648 to 2147483647)

Default Configuration

0 is the default value.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the ip irdp preference to 1000 for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip irdp preference 1000
```

show ip irdp

Use the **show ip irdp** command in Privileged EXEC mode to display the router discovery information for all interfaces, or for a specified interface.

Syntax

```
show ip irdp {vlan vlan-id | all}
```

- *vlan-id* — Valid VLAN ID
- **all** — Shows information for all interfaces.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example shows router discovery information for VLAN 15.

```
console#show ip irdp vlan 15

Interface  Ad Mode  Advertise Address Max Int Min Int Hold
Time Preference

-----
vlan15      Enable
224.0.0.1      600      450      1800      0
```


Routing Information Protocol Commands

This chapter explains the following commands:

- auto-summary
- default-information originate
- default-metric
- distance rip
- distribute-list out
- enable
- hostroutesaccept
- ip rip
- ip rip authentication
- ip rip receive version
- ip rip send version
- redistribute
- router rip
- show ip rip
- show ip rip interface
- show ip rip interface brief
- split-horizon

auto-summary

Use the **auto-summary** command in Router RIP Configuration mode to enable the RIP auto-summarization mode. Use the **no** form of the command to disable auto-summarization mode.

Syntax

auto-summary

no auto-summary

Default Configuration

Disabled is the default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-router)#auto-summary
```

default-information originate

Use the **default-information originate** command in Router RIP Configuration mode to control the advertisement of default routes.

Syntax

default-information originate

no default-information originate

Default Configuration

This command has no default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-router)#default-information originate
```

default-metric

Use the **default-metric** command in Router RIP Configuration mode to set a default for the metric of distributed routes. Use the **no** form of the command to return the metric to the default value.

Syntax

default-metric *integer*

no default-metric

- *integer* — Metric for the distributed routes. (Range: 1-15)

Default Configuration

Default metric is not configured by default.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets a default of 12 for the metric of distributed routes.

```
console(config-router)#default-metric 12
```

distance rip

Use the **distance rip** command in Router RIP Configuration mode to set the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route. Use the no form of the command to return the preference to the default value.

Syntax

distance rip *integer*

no distance rip

- *integer* — RIP route preference. (Range: 1-255)

Default Configuration

15 is the default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the route preference value of RIP in the router at 100.

```
console(config-router)#distance rip 100
```

distribute-list out

Use the **distribute-list out** command in Router RIP Configuration mode to specify the access list to filter routes received from the source protocol. Use the no form of the command to remove the access list from the specified source protocol.

Syntax

distribute-list *accesslistname* **out** {ospf | static | connected}

no distribute-list *accesslistname* **out** {**ospf** | **static** | **connected**}

- *accesslistname* — The name used to identify the existing ACL. The range is 1-31 characters.
- **ospf** — Apply the specific access list when OSPF is the source protocol.
- **static** — Apply the specified access list when packets come through a static route.
- **connected** — Apply the specified access list when packets come from a directly connected route.

Default Configuration

This command has no default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example elects access list ACL40 to filter routes received from the source protocol.

```
console(config-router)#distribute-list ACL40 out
static
```

enable

Use the **enable** command in Router RIP Configuration mode to reset the default administrative mode of RIP in the router (active). Use the no form of the command to disable the administrative mode for RIP.

Syntax

enable

no enable

Default Configuration

Enabled is the default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

```
console (config-router) #enable
```

hostroutesaccept

Use the **hostroutesaccept** command in Router RIP Configuration mode to enable the RIP hostroutesaccept mode. Use the no form of the command to disable the RIP hostroutesaccept mode.

Syntax

hostroutesaccept

no hostroutesaccept

Default Configuration

Enabled is the default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

```
console (config-router) #hostroutesaccept
```

ip rip

Use the **ip rip** command in Interface Configuration mode to enable RIP on a router interface. Use the no form of the command to disable RIP on the interface.

Syntax

ip rip

no ip rip

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-vlan2)#ip rip
```

```
console(config-if-vlan2)#no ip rip
```

ip rip authentication

Use the **ip rip authentication** command in Interface Configuration Mode to set the RIP Version 2 Authentication Type and Key for the specified interface. Use the no form of the command to return the authentication to the default value.

Syntax

ip rip authentication {none | {simple *key*} | {encrypt *key key-id*}}

no ip rip authentication

- *key* — Authentication key for the specified interface. (Range: 16 bytes or less)

- `encrypt` — Specifies the Ethernet unit/port of the interface to view information.
- `key-id` — Authentication key identifier for authentication type `encrypt`. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the RIP Version 2 Authentication Type and Key for VLAN 11.

```
console(config-if-vlan11)#ip rip authentication
encrypt pass123 35
```

ip rip receive version

Use the `ip rip receive version` command in Interface Configuration mode to configure the interface to allow RIP control packets of the specified version(s) to be received. Use the `no` form of the command to return the version to the default value.

Syntax

`ip rip receive version {rip1 | rip2 | both | none}`

`no ip rip receive version`

- `rip1` — Receive only RIP version 1 formatted packets.
- `rip2` — Receive only RIP version 2 formatted packets.
- `both` — Receive packets from either format.
- `none` — Do not allow any RIP control packets to be received.

Default Configuration

Both is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example allows no RIP control packets to be received by VLAN 11.

```
console(config-if-vlan11)#ip rip receive version none
```

ip rip send version

Use the **ip rip sent version** command in Interface Configuration mode to configure the interface to allow RIP control packets of the specified version to be sent. Use the no form of the command to return the version to the default value.

Syntax

ip rip send version {rip1 | rip1c | rip2 | none}

no ip rip send version

- rip1 — Send RIP version 1 formatted packets.
- rip1c — Send RIP version 1 compatibility mode, which sends RIP version 2 formatted packets via broadcast.
- rip2 — Send RIP version 2 using multicast.
- none — Do not allow any RIP control packets to be sent.

Default Configuration

RIP2 is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example allows no RIP control packets to be sent by VLAN 11.

```
console(config-if-vlan11)#ip rip send version none
```

redistribute

The **redistribute** command configures RIP protocol to redistribute routes from the specified source protocol/routers. If the source protocol is OSPF, there are five possible match options.

Syntax

```
redistribute ospf [metric integer] [match [internal] [external 1] [external 2]  
[nssa-external 1] [nssa-external 2]]
```

```
no redistribute ospf
```

```
redistribute { static | connected } [metric integer]
```

- metric *integer*— Specifies the metric to use when redistributing the route. Range: 0-15.
- match internal — Adds internal matches to any match types presently being redistributed.
- match external 1 — Adds routes imported into OSPF as Type-1 external routes into any match types presently being redistributed.
- match external 2 — Adds routes imported into OSPF as Type-2 external routes into any match types presently being redistributed.
- match nssa-external 1 — Adds routes imported into OSPF as NSSA Type-1 external routes into any match types presently being redistributed.
- match nssa-external 2 — Adds routes imported into OSPF as NSSA Type-2 external routes into any match types presently being redistributed.
- static — Redistributes static routes.

- `connected` — Redistributes directly-connected routes.

Default Configuration

`metric integer` — not configured

`match` — internal

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config-router)#redistribute ospf metric 10  
match nssa-external 1
```

```
console(config-router)#redistribute connected metric  
1
```

router rip

Use the `router rip` command in Global Configuration mode to enter Router RIP mode.

Syntax

`router rip`

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example enters Router RIP mode.

```
console(config)#router rip
console(config-router)#
```

show ip rip

Use the **show ip rip** command in Privileged EXEC mode to display information relevant to the RIP router.

Syntax

show ip rip

Default Configuration

The command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays information relevant to the RIP router.

```
console#show ip rip
RIP Admin Mode..... Enable
Split Horizon Mode..... Simple
Auto Summary Mode..... Enable
Host Routes Accept Mode..... Enable
Global route changes..... 0
Global queries..... 0
Default Metric..... 12
```

```

Default Route Advertise..... 0
Redistributing.....
Source..... Connected
Metric..... 2
Distribute List..... Not configured
Redistributing.....
Source..... ospf
Metric..... 10
Match Value..... 'nssa-external
1'
Distribute List..... Not configured

```

show ip rip interface

Use the **show ip rip interface** command in Privileged EXEC mode to display information related to a particular RIP interface.

Syntax

show ip rip interface *vlan *vlan-id**

- *vlan-id* — Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays information related to the VLAN 15 RIP interface.

```
console#show ip rip interface vlan 15
Interface..... 15
IP Address..... ----
Send version..... RIP-2
Receive version..... Both
RIP Admin Mode..... Disable
Link State..... ----
Authentication Type..... MD5
Authentication Key..... "pass123"
Authentication Key ID..... 35
Bad Packets Received..... ----
Bad Routes Received..... ----
Updates Sent..... ----
```

show ip rip interface brief

Use the **show ip rip interface brief** command in Privileged EXEC mode to display general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e. ip rip).

Syntax

```
show ip rip interface brief
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays general information for each RIP interface.

```
console#show ip rip interface brief
```

		Send	Receive	RIP	Link
Interface	IP Address	Version	Version	Mode	State
-----	-----	-----	-----	-----	-----
vlan1	0.0.0.0	RIP-2	Both	Disable	Down
vlan2	0.0.0.0	RIP-2	Both	Disable	Down

split-horizon

Use the **split-horizon** command in Router RIP Configuration mode to set the RIP split horizon mode. Use the no form of the command to return the mode to the default value.

Syntax

split-horizon {none | simple | poison}

no split-horizon

- none — RIP does not use split horizon to avoid routing loops.
- simple — RIP uses split horizon to avoid routing loops.
- poison — RIP uses split horizon with poison reverse (increases routing packet update size).

Default Configuration

Simple is the default configuration.

Command Mode

Router RIP Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example does not use split horizon.

```
console(config-router)#split-horizon none
```

Tunnel Interface Commands

This chapter explains the following commands:

- interface tunnel
- show interfaces tunnel
- tunnel destination
- tunnel mode ipv6ip
- tunnel source

interface tunnel

Use the **interface tunnel** command in Global Configuration mode to enter the interface configuration mode for a tunnel.

Syntax

interface tunnel *tunnel-id*

no interface tunnel *tunnel-id*

- *tunnel-id*— Tunnel identifier. (Range: 0–7)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example enables the interface configuration mode for tunnel 1.

```
console(config)#interface tunnel 1
```

```
console(config-if-tunnel1)#
```

show interfaces tunnel

Use the **show interfaces tunnel** command in Privileged EXEC mode to display the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.

Syntax

show interfaces tunnel [*tunnel-id*]

- *tunnel-id*— Tunnel identifier. (Range: 0–7)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Examples

The following examples show the parameters related to an individual tunnel and to all tunnel interfaces.

```
console#show interfaces tunnel 1
Interface Link Status..... down
MTU size..... 1480 bytes

console#show interfaces tunnel
TunnelId      Interface      TunnelMode  SourceAddress  Dest.Address
-----
1             tunnel 1      IPv6OVER4   10.254.25.14   10.254.25.10
2             tunnel 2      IPv6OVER4                   10.254.20.10
```

tunnel destination

Use the **tunnel destination** command in Interface Configuration mode to specify the destination transport address of the tunnel.

Syntax

tunnel destination *ipv4addr*

no tunnel destination

- *ipv4addr* — Valid ipv4 address.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Tunnel) mode.

User Guidelines

This command has no user guidelines.

Example

The following example specifies the destination transport address of tunnel 1.

```
console(config)#interface tunnel 1
console(config-if-tunnel1)#tunnel destination
10.1.1.1
```

tunnel mode ipv6ip

Use the **tunnel mode ipv6ip** command in Interface Configuration mode to specify the mode of the tunnel.

Syntax

tunnel mode ipv6ip [6to4]

no tunnel mode

- **6to4** — Sets the tunnel mode to automatic.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Tunnel) mode.

User Guidelines

This command has no user guidelines.

Example

The following example specifies ipv6ip mode for tunnel 1.

```
console(config)#interface tunnel 1
console(config-if-tunnel1)#tunnel mode ipv6ip
console(config-if-tunnel1)#tunnel mode ipv6ip 6to4
```

tunnel source

Use the **tunnel source** command in Interface Configuration mode to specify the source transport address of the tunnel, either explicitly or by reference to an interface.

Syntax

tunnel source {*ipv4addr* | *vlan vlan-id*}

no tunnel source

- *ipv4addr*— Valid ipv4 address.
- *vlan-id*— Valid VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Tunnel) mode.

User Guidelines

This command has no user guidelines.

Example

The following example specifies VLAN 11 as the source transport address of the tunnel.

```
console(config)#interface tunnel 1
console(config-if-tunnel1)#tunnel source vlan 11
```


Virtual LAN Routing Commands

This chapter explains the following command:

- `show ip vlan`

show ip vlan

Use the **show ip vlan** command in Privileged EXEC mode to display the VLAN routing information for all VLANs with routing enabled.

Syntax

show ip vlan

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays VLAN routing information.

```
console#show ip vlan
```

```
MAC Address used by Routing VLANs: 00:00:00:01:00:02
```

VLAN ID	IP Address	Subnet Mask
-----	-----	-----
10	0.0.0.0	0.0.0.0
20	0.0.0.0	0.0.0.0

Virtual Router Redundancy Protocol Commands

This chapter explains the following Virtual LAN routing commands:

- ip vrrp
- ip vrrp authentication
- ip vrrp ip
- ip vrrp mode
- ip vrrp preempt
- ip vrrp priority
- ip vrrp timers advertise
- ip vrrp track interface
- ip vrrp track ip route
- show ip vrrp
- show ip vrrp interface
- show ip vrrp interface brief
- show ip vrrp interface stats

ip vrrp

Use the **ip vrrp** command in Global Configuration mode to enable the administrative mode of VRRP for the router. In Interface Config mode, this command enables the VRRP protocol on an interface. Use the **no** form of the command to disable the administrative mode of VRRP for the router.

Syntax (Global Config Mode)

ip vrrp

no ip vrrp

Syntax (Interface Config Mode)

ip vrrp *vr-id*

no ip vrrp *vr-id*

- *vr-id* — Virtual router identification. (Range: 1-255)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration or Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example enables VRRP protocol on the router.

```
console(config)#ip vrrp
```

The following example in Interface Configuration mode enables VRRP protocol on VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip vrrp 5
```


ip vrrp authentication

Use the **ip vrrp authentication** command in Interface Configuration mode to set the authorization details value for the virtual router configured on a specified interface. Use the **no** form of the command to return the authentication type to the default value.

Syntax

ip vrrp *vr-id* authentication {none | simple *key*}

no ip vrrp *vr-id* authentication

- *vr-id*— The virtual router identifier. (Range: 1-255)
- none — Indicates authentication type is none.
- simple — Authentication type is a simple text password.
- *key*— The key for simple authentication. (Range: String values)

Default Configuration

None is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the authorization details value for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip vrrp 5 authentication
simple test123
```

ip vrrp ip

Use the **ip vrrp ip** command in Interface Configuration mode to set the virtual router IP address value for an interface. Use the **no** form of the command to remove the secondary IP address.



NOTE: In order to be configured on a routing interface, the VRRP IP address must belong to subnet(s) (Primary or Secondary) corresponding to the IP address (Primary/Secondary) configured on that routing interface, otherwise the CLI and Web interfaces will report an error message.

Syntax

ip vrrp *vr-id* **ip** *ip-address* [**secondary**]

no ip vrrp *vr-id* **ip** *ip-address* **secondary**

- *vr-id* — The virtual router identifier. (Range: 1-255)
- *ip-address* — The IP address of the virtual router.
- **secondary** — Designates the virtual router IP address as a secondary IP address on an interface.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

The primary IP address can be modified, but not deleted. The **no** form of the command is only valid for the secondary IP address.

Example

The following example sets the virtual router IP address for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip vrrp 5 ip 192.168.5.25
```

ip vrrp mode

Use the **ip vrrp mode** command in Interface Configuration mode to enable the virtual router configured on an interface. Enabling the status field starts a virtual router. Use the **no** form of the command to disable the virtual router.

Syntax

ip vrrp *vr-id* **mode**

no ip vrrp *vr-id* **mode**

- *vr-id*— The virtual router identifier. (Range: 1-255)

Default Configuration

Disabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example enables the virtual router for VLAN 15.

```
console(config)#interface vlan 15
```

```
console(config-if-vlan15)#ip vrrp 5 mode
```

ip vrrp preempt

Use the **ip vrrp preempt** command in Interface Configuration mode to set the preemption mode value for the virtual router configured on a specified interface. Use the **no** form of the command to disable preemption mode.

Syntax

ip vrrp *vr-id* **preempt**

no ip vrrp *vr-id* **preempt**

- *vr-id*— The virtual router identifier. (Range: 1-255)

Default Configuration

Enabled is the default configuration.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the preemption mode value for the virtual router for VLAN 15.

```
console(config)#interface vlan 15
console(config-if-vlan15)#ip vrrp 5 preempt
```

ip vrrp priority

Use the **ip vrrp priority** command in Interface Configuration mode to set the priority value for the virtual router configured on a specified interface. Use the no form of the command to return the priority to the default value.

Syntax

ip vrrp *vr-id* **priority** *priority*

no ip vrrp *vr-id* **priority**

- *vr-id*— The virtual router identifier. (Range: 1-255)
- *priority*— Priority value for the interface. (Range: 1-254)

Default Configuration

priority has a default value of 100.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the priority value for the virtual router for VLAN 15.

```
console(config-if-vlan15)#ip vrrp 5 priority 20
```

ip vrrp timers advertise

Use the **ip vrrp timers advertise** command in Interface Configuration mode to set the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement. Use the **no** form of the command to return the advertisement frequency to the default value.

Syntax

ip vrrp *vr-id* **timers advertise** *seconds*

no ip vrrp *vr-id* **priority**

- *vr-id*— The virtual router identifier. (Range: 1-255)
- *seconds*— The frequency at which an interface on the specified virtual router sends a virtual router advertisement. (Range: 1-255 seconds)

Default Configuration

seconds has a default value of 1.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the frequency at which the VLAN 15 virtual router sends a virtual router advertisement.

```
console(config-if-vlan15)#ip vrrp 5 timers advertise  
10
```

ip vrrp track interface

Use the **ip vrrp track interface** command to alter the priority of the VRRP router based on the availability of its interfaces. It is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up if IP on that interface is up. Otherwise, the tracked interface is down.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in priority argument. When the interface is up for IP protocol the priority will be incremented by the priority value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (default priority decrement) for each downed interface. The default priority decrement is changed using the priority argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default no interfaces are tracked. If we specify just the interface to be tracked without giving the priority, which is optional, then the default priority will be set.

Use the no form of this command to remove the interface from the tracked list or to restore the priority decrement to its default. When removing an interface from the tracked list, the priority is incremented by the decrement value if that interface is down.

Syntax

```
ip vrrp vrid track interface vlan vlan-id [decrement priority]
```

vrid—Virtual router identification (Range: 1–255).

vlan vlan-id—Valid VLAN ID.

priority—Priority decrement value for the tracked interface (Range: 1–254).

Default Configuration

No interfaces are tracked.

The default decrement priority is 10.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example adds VLAN 2 to the virtual router tracked list (with a priority decrement value of 20).

```
(config-if-vlan10)#ip vrrp 1 track interface vlan 2  
decrement 20
```

ip vrrp track ip route

Use the **ip vrrp track ip route** command to track the route reachability. When the tracked route is deleted, the priority of the VRRP router is decremented by the value specified in the priority argument. When the tracked route is added, the priority is incremented by the same. A VRRP configured interface can track more than one route. When a tracked route goes down, the priority of the router is decreased by 10 (default priority decrement) for each downed route. By default no routes are tracked. If we specify just the route to be tracked without giving the priority which is optional then the default priority will be set.

Use the “no” form of this command to remove the route from the tracked list or to restore the priority decrement to its default. When removing a tracked ip route from the tracked list, priority should be incremented by the decrement value if the route is not reachable.

Syntax

ip vrrp vrid track ip route *ip-address/prefix-length* [**decrement** *priority*]

vrid—Virtual router identification (Range: 1–255).

ip-address/prefix-length—Specifies the route to be tracked.

priority—Priority decrement value for the tracked route (Range: 1–254).

Default Configuration

There are no routes tracked by default.

The default decrement priority is 10.

Command Mode

Interface Configuration (VLAN) mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example adds the route 2.2.2.0/24 to the virtual router tracked list (with a priority decrement value of 20).

```
console(config-if-vlan10)#ip vrrp 1 track ip route  
2.2.2.0/24 decrement 20
```

show ip vrrp

Use the **show ip vrrp** command in Privileged EXEC mode to display whether VRRP functionality is enabled or disabled on the switch. The command also displays some global parameters which are required for monitoring.

Syntax

show ip vrrp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays VRRP's enabled status.

```
console#show ip vrrp
Admin Mode.....
Enable
Router Checksum Errors..... 0
Router Version Errors..... 0
Router VRID Errors..... 0
```

show ip vrrp interface

Use the **show ip vrrp interface** command in Privileged EXEC mode to display all configuration information and VRRP router statistics of a virtual router configured on a specific interface.

Syntax

show ip vrrp interface vlan *vlan-id* *vr-id*

- *vlan-id*— Valid VLAN ID.
- *vr-id*— The virtual router identifier. (Range: 1-255)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays all configuration information about the VLAN 15 virtual router.

```
console#show ip vrrp interface vlan 7 1
```

```

Primary IP Address..... 192.168.5.55
VMAC Address..... 0000.5E00.0101
Authentication Type..... None
Priority..... 60
Advertisement Interval (secs)..... 10
Pre-empt Mode..... Enable
Administrative Mode..... Enable
State..... Initialized

```

```

Track Interface State DecrementPriority
-----

```

```

vlan 3          Down    20

```

```

Track Route (pfx/len)    Reachable    DecrementPriority
-----

```

```

10.10.10.0/24          False        20

```

show ip vrrp interface brief

Use the **show ip vrrp interface brief** command in Privileged EXEC mode to display information about each virtual router configured on the switch. It displays information about each virtual router.

Syntax

```
show ip vrrp interface brief
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays all configuration information about the virtual router on the selected interface.

```
console#show ip vrrp interface brief
```

Interface	VRID	IP Address	Mode	State
-----	-----	-----	-----	-----
vlan1	2	0.0.0.0	Disable	Initialize
vlan2	5	192.168.5.55	Enable	Initialize

show ip vrrp interface stats

Use the **show ip vrrp interface stats** command in User EXEC mode to display the statistical information about each virtual router configured on the switch.

Syntax

```
show ip vrrp interface stats vlan vlan-id vr-id
```

- *vlan-id*— Valid VLAN ID.
- *vr-id*— The virtual router identifier. (Range: 1-255)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays all statistical information about the VLAN 15 virtual router.

```
console#show ip vrrp interface stats vlan 15 5
UpTime..... 0 days 0 hrs 0 mins 0 secs
Protocol..... IP
State Transitioned to Master..... 0
Advertisement Received..... 0
Advertisement Interval Errors..... 0
Authentication Failure..... 0
IP TTL Errors..... 0
Zero Priority Packets Received..... 0
Zero Priority Packets Sent..... 0
Invalid Type Packets Received..... 0
Address List Errors ..... 0
Invalid Authentication Type..... 0
Authentication Type Mismatch..... 0
Packet Length Errors..... 0
```

Autoconfig Commands

This chapter explains the following commands:

- boot host auto-save
- boot host dhcp
- boot host retry-count
- show boot

boot host auto-save

The **boot host auto-save** command enables/disables the option to automatically save configuration files downloaded to the switch by Auto Config.

Syntax

boot host auto-save

no boot host auto-save

Default Configuration

The downloaded configuration is not automatically saved by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines

Example

```
console#no boot host auto-save
```

boot host dhcp

The **boot host dhcp** command is used to enable/disable Auto Config on the switch.

Syntax

boot host dhcp

no boot host dhcp

Default Configuration

Auto Config is enabled.

Command Mode

Global Configuration.

User Guidelines

This command has no user guidelines

Example

```
console#no boot host dhcp
```

boot host retry-count

The **boot host retry-count** command sets the number of attempts to download a configuration. Use the "no" form of this command to reset the number to the default.

Syntax

```
boot host retry-count retry
```

```
no boot host retry-count
```

- *retry*—The number of attempts to download a configuration (Range: 1–6).

Default Configuration

The default number of configuration download attempts is three.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines

Example

```
console#boot host retry-count 5
```

show boot

The `show autoconfig` command displays the current status of the Auto Config process.

Syntax

`show boot`

Default Configuration

Not applicable

Command Mode

Privileged EXEC.

User Guidelines

This command has no user guidelines.

Example

```
console#show boot
```

```
Config Download
```

```
    via DHCP: enabled
```

```
Auto Config State   : Waiting for boot options
```

```
...
```

```
Auto Config State   : Resolving switch hostname
```

```
...
```

```
Auto Config State   : Downloading file <boot>.cfg
```


Captive Portal Commands

This chapter explains the following commands:

Captive Portal Global Commands

- authentication timeout
- captive-portal
- enable
- http port
- https port
- show captive-portal
- show captive-portal status

Captive Portal Configuration Commands

- block
- configuration
- enable
- group
- interface
- locale
- name
- protocol
- redirect
- redirect-url
- session-timeout
- verification

Captive Portal Client Connection Commands

- captive-portal client deauthenticate
- show captive-portal client status
- show captive-portal configuration client status

- show captive-portal interface client status
- show captive-portal interface configuration status

Captive Portal Interface Commands

- clear captive-portal users

Captive Portal Local User Commands

- clear captive-portal users
- no user
- show captive-portal user
- user group
- user name
- user password
- user session-timeout

Captive Portal Status Commands

- show captive-portal configuration
- show captive-portal configuration interface
- show captive-portal configuration locales
- show captive-portal configuration status
- show trapflags captive-portal

Captive Portal User Group Commands

- user group
- user group moveusers
- user group name

Captive Portal Global Commands

authentication timeout

Use the **authentication timeout** command to configure the authentication timeout. If the user does not enter valid credentials within this time limit, the authentication page needs to be served again in order for the client to gain access to the network. Use the “no” form of this command to reset the authentication timeout to the default.

Syntax

authentication timeout *timeout*

no authentication timeout

- *timeout*—The authentication timeout (Range: 60–600 seconds).

Default Configuration

The default authentication timeout is 300 seconds.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP)#authentication timeout 600
console(config-CP)#no authentication timeout
```

captive-portal

Use the **captive-portal** command to enter the captive portal configuration mode.

Syntax

`captive-portal`

Default Configuration

There is no default configuration for this command.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console (config) #captive-portal
```

```
console (config-CP) #
```

enable

Use the **enable** command to globally enable captive portal. Use the “no” form of this command to globally disable captive portal.

Syntax

`enable`

`no enable`

Default Configuration

Captive Portal is disabled by default.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP)#enable
```

http port

Use the **http port** command to configure an additional HTTP port for captive portal to monitor. Use the “no” form of this command to remove the additional HTTP port from monitoring.

Syntax

```
http port port-num
```

```
no http port
```

- *port-num*—The port number to monitor (Range: 1–65535).

Default Configuration

Captive portal only monitors port 80 by default.

Command Mode

Captive Portal Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP)#http port 81
```

```
console(config-CP)#no http port
```

https port

Use the **https port** command to configure an additional HTTPS port for captive portal to monitor. Use the “no” form of this command to remove the additional HTTPS port from monitoring.

Syntax

```
https port port-num
```

no https port

- *port-num*—The port number to monitor (Range: 1–65535).

Default Configuration

Captive portal only monitors port 443 by default.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP)#https port 1443
```

```
console(config-CP)#no https port
```

show captive-portal

Use the **show captive-portal** command to display the status of the captive portal feature.

Syntax

show captive-portal

Default Configuration

There is no default configuration for this command

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal
Administrative Mode..... Disabled
Operational Status..... Disabled
Disable Reason..... Administrator Disabled
Captive Portal IP Address.... 1.2.3.4
```

show captive-portal status

Use the **show captive-portal status** command to report the status of all captive portal instances in the system.

Syntax

```
show captive-portal status
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal status

Additional HTTP Port..... 81
Additional HTTP Secure Port..... 1443
Authentication Timeout..... 300
Supported Captive Portals..... 10
```

Configured Captive Portals.....	1
Active Captive Portals.....	0
Local Supported Users.....	128
Configured Local Users.....	3
System Supported Users.....	1024
Authenticated Users.....	0

Captive Portal Configuration Commands

The commands in this section are related to captive portal configurations.

block

Use the **block** command to block all traffic for a captive portal configuration. Use the “no” form of this command to unblock traffic.

Syntax

block

no block

Default Configuration

Traffic is not blocked by default.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#block
```


configuration

Use the **configuration** command to enter the captive portal instance mode. The captive portal configuration identified by CP ID 1 is the default CP configuration. The system supports a total of ten CP configurations. Use the “no” form of this command to delete a configuration. The default configuration cannot be deleted.

Syntax

configuration *cp-id*

no configuration *cp-id*

- *cp-id*—Captive Portal ID (Range: 1–10).

Default Configuration

There is no default configuration for this command.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console (config-CP) #configuration 2
```

```
console (config-CP 2) #
```

enable

Use the **enable** command to enable a captive portal configuration. Use the “no” form of this command to disable a configuration.

Syntax

enable

no enable

Default Configuration

Configurations are enabled by default

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#no enable
```

group

Use the **group** command to configure the group number for a captive portal configuration. If a group number is configured, the user entry (Local or RADIUS) must be configured with the same name and the group to authenticate to this captive portal instance. Use the “no” form of this command to reset the group number to the default.

Syntax

group *group-number*

no group

- *group-number*—The number of the group to associate with this configuration (Range: 1–10).

Default Configuration

The default group number is 1.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#group 2
```

interface

Use the **interface** command to associate an interface with a captive portal configuration. Use the “no” form of this command to remove an association.

Syntax

```
interface interface
```

```
no interface interface
```

interface—An interface or range of interfaces.

Default Configuration

No interfaces are associated with a configuration by default.

Command Mode

Captive Portal Instance Config mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#interface 1/g2
```

locale

The **locale** command is not intended to be a user command. The administrator must use the Web UI to create and customize captive portal web content. This command is primarily used by the show running-config command and process as it provides the ability to save and restore configurations using a text based format.

Syntax

```
locale web-id
```

- *web-id*—The locale number (Range: Only locale 1 is supported)

Default Configuration

Locale 1 is configured by default.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

name

Use the **name** command to configure the name for a captive portal configuration. Use the “no” form of this command to remove a configuration name.

Syntax

name *cp-name*

no name

- *cp-name*—CP configuration name (Range: 1–32 characters).

Default Configuration

Configuration 1 has the name “Default” by default. All other configurations have no name by default.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#name cp2
```

protocol

Use the **protocol** command to configure the protocol mode for a captive portal configuration.

Syntax

protocol {http | https}

Default Configuration

The default protocols mode is https.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#protocol http
```

redirect

Use the **redirect** command to enable the redirect mode for a captive portal configuration. Use the “no” form of this command to disable redirect mode.

Syntax

redirect

no redirect

Default Configuration

Redirect mode is disabled by default.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#redirect
```

redirect-url

Use the **redirect-url** command to configure the redirect URL for a captive portal configuration.

Syntax

redirect-url *url*

- *url*—The URL for redirection (Range: 1–512 characters).

Default Configuration

There is no redirect URL configured by default.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#redirect-url www.dell.com
```

session-timeout

Use the **session-timeout** command to configure the session timeout for a captive portal configuration. Use the “no” form of this command to reset the session timeout to the default.

Syntax

session-timeout *timeout*

no session-timeout

- *timeout*—Session timeout. 0 indicates timeout not enforced (Range: 0–86400 seconds).

Default Configuration

There is no session timeout by default.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#session-timeout 86400
console(config-CP 2)#no session-timeout
```

verification

Use the **verification** command to configure the verification mode for a captive portal configuration.

Syntax

verification {**guest** | **local** | **radius**}

- **guest**—Allows access for unauthenticated users (users that do not have assigned user names and passwords).
- **local**—Authenticates users against a local user database.
- **radius**—Authenticates users against a remote RADIUS database.

Default Configuration

The default verification mode is **guest**.

Command Mode

Captive Portal Instance mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP 2)#verification local
```

Captive Portal Client Connection Commands

captive-portal client deauthenticate

Use the **captive-portal client deauthenticate** command to deauthenticate a specific captive portal client.

Syntax

captive-portal client deauthenticate *macaddr*

- *macaddr*—Client MAC address.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#captive-portal client deauthenticate 0002.BC00.1290
```

show captive-portal client status

Use the **show captive-portal client status** command to display client connection details or a connection summary for connected captive portal users.

Syntax

show captive-portal client [*macaddr*] status

- *macaddr*—Client MAC address.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal client status
Client MAC Address Client IP Address Protocol Verification
Session Time
-----
0002.BC00.1290      10.254.96.47      https      Local
0d:00:01:20
0002.BC00.1291      10.254.96.48      https      Local
0d:00:05:20
0002.BC00.1292      10.254.96.49      https      Radius
0d:00:00:20

console#show captive-portal client 0002.BC00.1290 status
Client MAC Address..... 0002.BC00.1290
Client IP Address..... 10.254.96.47
Protocol Mode..... https
Verification Mode..... Local
CP ID..... 1
```

```
CP Name..... cp1
Interface..... 1/g1
Interface Description..... Unit: 1 Slot: 0
Port: 1 Gigabit - Level
User Name..... user123
Session Time..... 0d:00:00:13
```

show captive-portal configuration client status

Use the `show captive-portal configuration client status` command to display the clients authenticated to all captive portal configurations or a to specific configuration.

Syntax

`show captive-portal configuration [cp-id] client status`

- *cp-id*—Captive Portal ID.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal configuration client status
CP ID      CP Name      Client MAC Address Client IP Address
Interface
-----
-----
1          cp1          0002.BC00.1290      10.254.96.47
1/g1
```

1/g2		0002.BC00.1291	10.254.96.48
2	cp2	0002.BC00.1292	10.254.96.49
1/g3			
3	cp3	0002.BC00.1293	10.254.96.50
1/g4			

```
console#show captive-portal configuration 1 client status
```

```
CP ID..... 1
```

```
CP Name..... cp1
```

Client	Client		
MAC Address	IP Address	Interface	Interface
Description			
-----	-----	-----	-----

0002.BC00.1290	10.254.96.47	1/g1	Unit: 1 Slot: 0
Port: 1 Gigabit			
0002.BC00.1291	10.254.96.48	1/g2	Unit: 1 Slot: 0
Port: 2 Gigabit			

show captive-portal interface client status

Use the `show captive-portal interface client status` command to display information about clients authenticated on all interfaces or a specific interface.

Syntax

```
show captive-portal interface interface client status
```

- *interface*—A valid interface in unit/port format.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal interface client status
```

Intf Address	Intf Description	Client MAC Address	Client IP
1/g1	Unit: 1 Slot: 0 Port: 1 Gigabit	0002.BC00.1290	
10.254.96.47			
		0002.BC00.1291	
10.254.96.48			
1/g2	Unit: 1 Slot: 0 Port: 2 Gigabit	0002.BC00.1292	
10.254.96.49			
1/g3	Unit: 1 Slot: 0 Port: 3 Gigabit	0002.BC00.1293	
10.254.96.50			

```
console#show captive-portal interface 1/g1 client status
Interface..... 1/g1
Interface Description..... Unit: 1 Slot: 0 Port: 1
Gigabit
```

Client MAC Address	Client IP Address	CP ID	CP Name	Protocol
Verification				
-----0002.BC00.1290	10.254.96.47	1	cp1	
http local				
0002.BC00.1291	10.254.96.48	2	cp2	http
local				

Captive Portal Interface Commands

show captive-portal interface configuration status

Use the `show captive-portal interface configuration status` command to display the interface to configuration assignments for all captive portal configurations or for a specific configuration.

Syntax

`show captive-portal interface configuration [cp-id] status`

- *cp-id*—Captive Portal ID.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal interface configuration status
```

CP ID	CP Name	Interface	Interface Description
Type			

1	Default	1/g1	Unit: 1 Slot: 0 Port: 1 Gigabit
...	Physical		

```
console#show captive-portal interface configuration 1 status
```

```
CP ID..... 1
CP Name..... cpl
```

Interface	Interface Description	Type

1/g1	Unit: 1 Slot: 0 Port: 1 Gigabit ...	Physical

Captive Portal Local User Commands

clear captive-portal users

Use the `clear captive-portal users` command to delete all captive portal user entries.

Syntax

`clear captive-portal users`

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#clear captive-portal users
```

no user

Use the `no user` command to delete a user from the local user database. If the user has an existing session, it is disconnected.

Syntax

`no user user-id`

- user-id*—User ID (Range: 1–128).

Default Configuration

There is no default configuration for this command.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console (config-CP) #no user 1
```

show captive-portal user

Use the **show captive-portal user** command to display all configured users or a specific user in the captive portal local user database.

Syntax

show captive-portal user [user-id]

- *user-id*—User ID (Range: 1–128).

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal user
```

Session

User ID	User Name	Timeout	Group ID	Group Name
---------	-----------	---------	----------	------------

1	user123	14400	1	Default
2	user234	0	1	Default
			2	group2

```
console#show captive-portal user 1
```

```
User ID..... 1
User Name..... user123
Password Configured..... Yes
Session Timeout..... 0
```

Group ID	Group Name
1	Default
2	group2

user group

Use the **user group** command to associate a group with a captive portal user. Use the “no” form of this command to disassociate a group and user. A user must be associated with at least one group so the last group cannot be disassociated.

Syntax

user *user-id* **group** *group-id*

- *user-id*—User ID (Range: 1–128).
- *group-id*—Group ID (Range: 1–10).

Default Configuration

A user is associated with group 1 by default.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP)#user 1 group 3
```

user name

Use the **user name** command to modify the user name for a local captive portal user.

Syntax

user *user-id* **name** *name*

- *user-id*—User ID (Range: 1–128).
- *name*—user name (Range: 1–32 characters).

Default Configuration

There is no name for a user by default.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines.

Example

```
console(config-CP)#user 1 name johnsmith
```

user password

Use the **user password** command to create a local user or change the password for an existing user.

Syntax

user *user-id* **password** {*password* | **encrypted** *enc-password*}

- *user-id*—User ID (Range: 1–128).
- *password*—User password (Range: 8–64 characters).
- *enc-password*—User password in encrypted form.

Default Configuration

There are no users configured by default.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(Config-CP)#user 1 password
Enter password (8 to 64 characters): *****
Re-enter password: *****
```

user session-timeout

Use the **user session-timeout** command to set the session timeout value for a captive portal user. Use the “no” form of this command to reset the session timeout to the default.

Syntax

user *user-id* **session-timeout** *timeout*

no user *user-id* **session-timeout**

- *user-id*—User ID (Range: 1–128).
- *timeout*—Session timeout. 0 indicates use global configuration (Range: 0–86400 seconds).

Default Configuration

The global session timeout is used by default.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP)#user 1 session-timeout 86400
console(config-CP)#no user 1 session-timeout
```

Captive Portal Status Commands

show captive-portal configuration

Use the **show captive-portal configuration** command to display the operational status of each captive portal configuration.

Syntax

show captive-portal configuration *cp-id*
cp-id—Captive Portal ID.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal configuration 1
CP ID..... 1
CP Name..... cp1
```

```
Operational Status..... Disabled
Disable Reason..... Administrator Disabled
Blocked Status..... Not Blocked
Authenticated Users..... 0
```

show captive-portal configuration interface

Use the `show captive-portal configuration interface` command to display information about all interfaces assigned to a captive portal configuration or about a specific interface assigned to a captive portal configuration.

Syntax

`show captive-portal configuration cp-id interface [interface]`

- *cp-id*—Captive Portal ID.
- *interface*—Interface in unit/port format.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal configuration 1 interface
CP ID..... 1
CP Name..... cp1
```

		Operational	Block
Interface	Interface Description	Status	
Status			

```

-----
-----
1/g1 Unit: 1 Slot: 0 Port: 1 Gigabit - Level Disabled      Blocked

console#show captive-portal configuration 1 interface 1/g1
CP ID..... 1
CP Name..... cp1
Interface..... 1/g1
Interface Description..... Unit: 1 Slot: 0
Port: 1 Gigab...
Operational Status..... Disabled
Disable Reason..... Interface Not
                        Attached
Block Status..... Not Blocked
Authenticated Users..... 0

```

show captive-portal configuration locales

Use the `show captive-portal configuration locales` command to display locales associated with a specific captive portal configuration.

Syntax

`show captive-portal configuration cp-id locales`

- *cp-id*—Captive Portal Configuration ID.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal configuration 1 locales
```

```
Locale Code
-----
en
```

show captive-portal configuration status

Use the `show captive-portal configuration status` command to display information about all configured captive portal configurations or about a specific captive portal configuration.

Syntax

```
show captive-portal configuration [cp-id] status
```

- *cp-id*—Captive Portal ID.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show captive-portal configuration status
```

CP ID	CP Name	Mode	Protocol	Verification
1	cp1	Enable	https	Guest
2	cp2	Enable	http	Local
3	cp3	Disable	https	Guest

```
console#show captive-portal configuration 1 status
CP ID..... 1
CP Name..... cp1
Mode..... Enabled
Protocol Mode..... https
Verification Mode..... Guest
Group Name..... group123
Redirect URL Mode..... Enabled
Redirect URL..... www.cnn.com
Session Timeout (seconds)..... 86400
```

show trapflags captive-portal

Use the `show trapflags captive-portal` command to display which captive portal traps are enabled.

Syntax

```
show trapflags captive-portal
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console#show trapflags captive-portal
```

```
Client Authentication Failure Traps..... Disable
Client Connection Traps..... Disable
```

Client Database Full Traps..... Disable
Client Disconnection Traps..... Disable

Captive Portal User Group Commands

user group

Use the **user group** command to create a user group. Use the “no” form of this command to delete a user group. The default user group (1) cannot be deleted.

Syntax

user group *group-id*

no user group *group-id*

group-id—Group ID (Range: 1–10).

Default Configuration

User group 1 is created by default and cannot be deleted.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP)#user group 2
```

```
console(config-CP)#no user group 2
```


user group moveusers

Use the `user group moveusers` command to move a group's users to a different group.

Syntax

`user group group-id moveusers new-group-id`

- *group-id*—Group ID (Range: 1–10).
- *new-group-id*—Group ID (Range: 1–10).

Default Configuration

There is no default configuration for this command.

Command Mode

Captive Portal Configuration mode

User Guidelines

The new group-id must already exist.

Example

```
console(config-CP)#user group 2 moveusers 3
```

user group name

Use the `user group name` command to configure a group name.

Syntax

`user group group-id name name`

- *group-id*—Group ID (Range: 1–10).
- *name*—Group name (Range: 1–32 characters).

Default Configuration

User groups have no names by default.

Command Mode

Captive Portal Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-CP)#user group 2 name group2
```

Clock Commands

This chapter explains the following commands:

- `show clock`
- `show sntp configuration`
- `show sntp status`
- `sntp authenticate`
- `sntp authentication-key`
- `sntp broadcast client enable`
- `sntp client poll timer`
- `sntp server`
- `sntp trusted-key`
- `sntp unicast client enable`
- `clock timezone hours-offset`
- `no clock timezone`
- `clock summer-time recurring`
- `clock summer-time date`
- `no clock summer-time`
- `show clock`

show clock

Use the `show clock` command in User EXEC mode to display the time and date from the system clock.

Syntax

`show clock`

Default Configuration

This command has no default setting.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays the time and date from the system clock

```
console>show clock
```

```
15:29:03 Jun 17 2002
```

```
Time source is SNTP
```

show sntp configuration

Use the **show sntp configuration** command in Privileged EXEC mode to show the configuration of the Simple Network Time Protocol (SNTP).

Syntax

```
show sntp configuration
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the current SNTP configuration of the device.

```
console#show sntp configuration
```

Polling interval: 64 seconds

MD5 Authentication keys:

Authentication is not required for synchronization.

Trusted keys:

No trusted keys.

Unicast clients: Disable

Unicast servers:

Server	Key	Polling	Priority
-----	-----	-----	-----

10.27.128.21	Disabled	Enabled	1

show sntp status

Use the `show sntp status` command in Privileged EXEC mode to show the status of the Simple Network Time Protocol (SNTP).

Syntax

`show sntp status`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example shows the status of the SNTP.

console#show sntp status

Client Mode: Unicast
Last Update Time: MAR 30 21:21:20 2009

Unicast servers:

Server	Status	Last response
-----	-----	-----

192.168.0.1	Up	21:21:20 Mar 30 2009

sntp authenticate

Use the **sntp authenticate** command in Global Configuration mode to require server authentication for received Network Time Protocol (NTP) traffic. To disable the feature, use the **no** form of this command.

Syntax

sntp authenticate
no sntp authenticate

Default Configuration

No authentication.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both Unicast and Broadcast.

Example

The following example, after defining the authentication key for SNTP, grants authentication.

```
console(config)# sntp authentication-key 8 md5 ClkKey
console(config)# sntp trusted-key 8
console(config)# sntp authenticate
```

sntp authentication-key

Use the **sntp authentication-key** command in Global Configuration mode to define an authentication key for Simple Network Time Protocol (SNTP). To remove the authentication key for SNTP, use the **no** form of this command.

Syntax

sntp authentication-key *key-number* md5 *value*

no sntp authentication-key *number*

- *key-number* — number (Range: 1–4294967295)
- *value* — value (Range: 1-8 characters)

Default value

No authentication is defined.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Examples

The following examples define the authentication key for SNTP.

```
console(config)# sntp authentication-key 8 md5 ClkKey
console(config)# sntp trusted-key 8
```

```
console(config)# sntp authenticate
```

sntp broadcast client enable

Use the **sntp broadcast client enable** command in Global Configuration mode to enable a Simple Network Time Protocol (SNTP) Broadcast client. To disable an SNTP Broadcast client, use the **no** form of this command.

Syntax

```
sntp broadcast client enable
```

```
no sntp broadcast client enable
```

Default Configuration

The SNTP Broadcast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables a Simple Network Time Protocol (SNTP) Broadcast client.

```
console(config)# sntp broadcast client enable
```

sntp client poll timer

Use the **sntp client poll timer** command in Global Configuration mode to set the polling time for the Simple Network Time Protocol (SNTP) client. To return to the default settings, use the **no** form of this command.

Syntax

```
sntp client poll timer seconds
```

```
no sntp client poll timer
```


- *seconds* — Polling interval. (Range: 64-1024 seconds, in powers of 2)

Default Configuration

The polling interval is 64 seconds.

Command Mode

Global Configuration mode

User Guidelines

If a user enters a value which is not an exact power of two, the nearest power-of-two value is applied.

Example

The following example sets the polling time for the Simple Network Time Protocol (SNTP) client to 1024 seconds.

```
console(config)# sntp client poll timer 1024
```

sntp server

Use the **sntp server** command in Global Configuration mode to configure the device to use Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from a specified server. To remove a server from the list of SNTP servers, use the **no** form of this command.

Syntax

sntp server {*ip-address* | *hostname*} [**priority** *priority*] [**poll**] [**key** *key-number*]

no sntp server *ip-address*

- *ip-address* — IP address of the server.
- *hostname* — Hostname of the server. (Range: 1-158 characters)
- **poll** — Enables polling.
- *key-number* — Authentication key to use when sending packets to this peer.
(Range: 1-4294967295)

- *priority* — Priority assigned to the server. (Range: 1–8)

Default Configuration

No servers are defined.

Command Mode

Global Configuration mode

User Guidelines

Up to 8 SNTP servers can be defined.

Use the **sntp client enable** command in Global Configuration mode to enable unicast clients globally.

Polling time is determined by the **sntp client poll timer <64-1024> global** configuration command.

Example

The following example configures the device to accept Simple Network Time Protocol (SNTP) traffic from the server at IP address 192.1.1.1.

```
console(config)# sntp server 192.1.1.1
```

sntp trusted-key

Use the **sntp trusted-key** command in Global Configuration mode to authenticate the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize. To disable authentication of the identity of the system, use the **no** form of this command.

Syntax

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

- *key-number* — Key number of authentication key to be trusted. (Range: 1–4294967295)

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

This command is relevant for both received Unicast and Broadcast.

Example

The following defines SNTP trusted-key.

```
console(config)# sntp authentication-key 8 md5 ClkKey
console(config)# sntp trusted-key 8
console(config)# sntp authenticate
```

sntp unicast client enable

Use the **sntp unicast client enable** command in Global Configuration mode to enable a client to use Simple Network Time Protocol (SNTP) predefined Unicast clients. To disable an SNTP Unicast client, use the **no** form of this command.

Syntax

```
sntp unicast client enable
no sntp unicast client enable
```

Default Configuration

The SNTP Unicast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp server** command to define SNTP servers.

Examples

The following example enables the device to use Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers.

```
console(config)# sntp unicast client enable
```

clock timezone hours-offset

Use the **clock timezone** [**hours-offset**] [**minutes** *minutes-offset*] [**zone** *acronym*] command to set the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either '0' or '\0', as appropriate.

Syntax

clock timezone hours-offset [**minutes** *minutes-offset*] [**zone** *acronym*]

- *hours-offset* — Hours difference from UTC. (Range: -12 to +13)
- *minutes-offset* — Minutes difference from UTC. (Range: 0-59)
- *acronym* — The acronym for the time zone. (Range: Up to four characters)

Command Mode

Global Configuration

Default Value

No default setting

User Guidelines

No specific guidelines

Example

```
console(config)#clock timezone -5 minutes 30 zone IST
```

no clock timezone

Use the **no clock timezone** command to reset the time zone settings.

Syntax

no clock timezone

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

This command has no specific user guidelines.

Example

```
console(config)#no clock timezone
```

clock summer-time recurring

Use the **clock summer-time recurring** {usa | eu | {week day month hh:mm week day month hh:mm}} [offset offset] [zone acronym] command to set the summertime offset to UTC recursively every year. If the optional parameters are not specified, they are read as either '0' or '\0', as appropriate.

Syntax

clock summer-time recurring {usa | eu | {week day month hh:mm week day month hh:mm}} [offset offset] [zone acronym]

- *week* — Week of the month. (Range: 1–5, first, last)
- *day* — Day of the week. (Range: The first three letters by name; sun, for example.)
- *month* — Month. (Range: The first three letters by name; jan, for example.)
- *hh:mm* — Time in 24-hour format in hours and minutes. (Range: hh: 0–23, mm: 0–59)
- *offset* — Number of minutes to add during the summertime. (Range: 1–1440)

- *acronym* — The acronym for the time zone to be displayed when summertime is in effect. (Range: Up to four characters)

Default Value

No default setting

Command Mode

Global Configuration

User Guidelines

No specific guidelines

Examples

```
console(config)# clock summer-time recurring 1 sun jan
00:10 2 mon mar 10:00 offset 1 zone ABC
```

clock summer-time date

Use the `clock summer-time date {date | month} {month | date} year hh:mm {date | month} {month | date} year hh:mm [offset offset] [zone acronym]` command to set the summertime offset to UTC. If the optional parameters are not specified, they are read as either '0' or '\0', as appropriate.

Syntax

`clock summer-time date {date | month} {month | date} year hh:mm {date | month} {month | date} year hh:mm [offset offset] [zone acronym]`

- *date* — Day of the month. (Range: 1–31)
- *month* — Month. (Range: The first three letters by name; jan, for example.)
- *year* — Year. (Range: 2000–2097)
- *hh:mm* — Time in 24-hour format in hours and minutes. (Range: hh: 0–23, mm: 0–59)
- *offset* — Number of minutes to add during the summertime. (Range: 1–1440)

- *acronym* — The acronym for the time zone to be displayed when summertime is in effect. (Range: Up to four characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

No specific guidelines

Examples

```
console(config)# clock summer-time date 1 Apr 2007  
02:00 28 Oct 2007 offset 90 zone EST
```

or

```
console(config)# clock summer-time date Apr 1 2007  
02:00 Oct 28 2007 offset 90 zone EST
```

no clock summer-time

Use the `no clock summer-time` command to reset the summertime configuration.

Syntax Description

`no clock summer-time`

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

No specific guidelines

Example

```
console(config)#no clock summer-time
```

show clock

Use the **show clock** command to display the time and date from the system clock. Use the **show clock detail** command to show the time zone and summertime configuration.

Syntax Description

show clock [detail]

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

No specific guidelines

Example

The following example shows the time and date only.

```
console# show clock
15:29:03 PDT(UTC-7) Jun 17 2005
Time source is SNTP
```

The following example shows the time, date, timezone, and summertime configuration.

```
console# show clock detail
15:29:03 PDT(UTC-7) Jun 17 2005
```


Time source is SNTP

Time zone:

Acronym is PST

Offset is UTC-7

Summertime:

Acronym is PDT

Recurring every year.

Begins at first Sunday of April at 2:00.

Ends at last Sunday of October at 2:00.

Offset is 60 minutes.

Configuration and Image File Commands

This chapter explains the following commands:

- boot system
- clear config
- copy
- delete backup-config
- delete backup-image
- delete startup-config
- filedescr
- script apply
- script delete
- script list
- script show
- script validate
- show backup-config
- show bootvar
- show dir
- show running-config
- show startup-config
- update bootcode

boot system

Use the **boot system** command in Privileged EXEC mode to specify the system image that the device loads at startup.

Syntax

boot system [image1 | image2]

- image1 | image2 — Image file.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show bootvar** command to find out which image is the active image.

Example

The following example loads system image **image1** for the next device startup.

```
console# boot system image1
```

clear config

Use the **clear config** command in Privileged EXEC mode to restore the switch to the default configuration.

Syntax

clear config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example restores the switch to its default configuration.

```
console#clear config
```

copy

Use the **copy** command in Privileged EXEC mode to copy files from a source to a destination.

Syntax

```
copy source-url destination-url {xmodem | tftp://ipaddr/filepath/filename |  
sftp|scp://username@ipaddr/filepath/filename | hostname |
```

```
copy ftp ftp://ipaddr/filepath/filename image}
```

- *source-url* — The location URL or reserved keyword of the source file being copied. (Range: 1–160 characters.)
- *destination-url* — The URL or reserved keyword of the destination file. (Range: 1–160 characters.)
- *ipaddr* — The IPv4 or IPv6 address of the server.
- *hostname* — Hostname of the server. (Range: 1–158 characters)
- *filepath* — The path to the file on the server.
- *filename* — The name of the file on the server.
- *username* — The user name for logging into the remote server via SSH.

The following table lists and describes reserved keywords.

Reserved Keyword	Description
running-config	Represents the current running configuration file.

Reserved Keyword	Description
startup-config	Represents the startup configuration file.
startup-log	Represents the startup syslog file. This can only be the source of a copy operation.
operational-log	Represents the operational syslog file. This can only be the source of a copy operation.
script <i>scriptname</i>	Represents a CLI script file.
image	Represents the software image file. When "image" is the target of a copy command, it refers to the backup image. When "image" is the source of a copy command, it refers to the active image. If this is destination, the file will be distributed to all units in the stack.
ftp:	Source or destination URL for an FTP network server. The syntax for this alias is <code>ftp://ipaddr/filepath/filename image</code> .
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is <code>tftp:[[/location]/directory]/filename</code> . An out-of-band IP address can be specified as described in the User Guidelines.
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
backup-config	Represents the backup configuration file.
unit	Indicates which unit in the stack is the target of the copy command.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The location of a file system dictates the format of the source or destination URL.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

Understanding Invalid Combinations of Source and Destination

Some combinations of source and destination are not valid. Specifically, if the following conditions exist, you can not use the **copy** command:

- If the source file and destination file are defined to be the same.
- **xmodem** cannot be a source and destination for the same copy operation. **xmodem** can only be copied to **image**.
- **tftp** cannot be the source and destination for the same copy operation.

The following topics contain copy character descriptions.

Copying Image File from a Server to Flash Memory

Use the **copy source-url image** command to copy an image file from a server to flash memory. Use the **boot system** command to activate the new image.

Copying a Configuration File from a Server to the Running Configuration

Use the **copy source-url running-config** command to load a configuration file from a network server to the device running configuration. The configuration is added to the running configuration as if the commands were typed in the command-line interface (CLI). The resulting configuration file is a combination of the previous running configuration and the loaded configuration file, with the loaded configuration file having precedence.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy source-url startup-config** command to copy a configuration file from a network server to the device startup configuration. These commands replace the startup configuration file with the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy running-config destination-url** command to copy the current configuration file to a network server using TFTP. Use the **copy startup-config destination-url** command to copy the startup configuration file to a network server.

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the `copy running-config startup-config` command to copy the running configuration to the startup configuration.

Backing up the Running Configuration or Startup Configuration to the Backup Configuration

Use the `copy running-config backup-config` command to back up the running configuration to the backup configuration file. Use the `copy startup-config backup-config` command to back up the startup configuration to the backup configuration file.

Copying to a Unit on the Stack Using unit

The `copy` command can be used to copy an image to another unit. This means that a `copy` command allows the management node to distribute its existing code to other nodes. The command syntax is `copy image unit {all | <1-12>}`



NOTE: The `copy` command can accept the `unit {all | <1-12>}` only as the destination-url. In this case, only **image** can be the source-url.



NOTE: The `copy image unit all` command does not copy the active image to the backup image on the management unit, just the stack units.

The `copy` command cannot:

- Either download code from tftp, for example, to the stack units directly, or
- Copy code from one stack unit to another stack unit.

For copying to all units simultaneously, use the keyword **all**.

Example

```
copy scp://user@serverip/PC6200v3.0.0.13.stk image
```

```
Remote Password:*****
```

delete backup-config

Use the `delete backup-config` command in Privileged EXEC mode to delete the backup-config file.

Syntax

`delete backup-config`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example deletes the backup-config file.

```
console#delete backup-config
```

```
Delete backup-config (Y/N)?y
```

delete backup-image

Use the `delete backup-image` command in Privileged EXEC mode to delete a file from a flash memory device.

Syntax

`delete backup-image`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Note that the active image cannot be deleted.

Example

The following example deletes test file in Flash memory.

```
console#delete backup-image
```

```
Delete: image2 (y/n)?
```

delete startup-config

Use the **delete startup-config** command in Privileged EXEC mode to delete the startup-config file.

Syntax

```
delete startup-config
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If the startup-config file is not present when system reboots, it reboots with default settings.

Example

The following example deletes the startup-config file.

```
console# delete startup-config
```

```
Delete startup-config (y/n)?
```

filedescr

Use the **filedescr** command in Privileged EXEC mode to add a description to a file. Use the **no** version of this command to remove the description from the filename.

Syntax

`filedescr {image 1 | image2} description`

`no filedescr {image 1 | image2}`

- `image1 | image2` — Image file.
- *description* — Block of descriptive text. (Range: 0-128 characters)

Default Configuration

No description is attached to the file.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example attaches a file description to image2.

```
console#filedescr image2 "backedup on 03-22-05"
```

script apply

Use the **script apply** command in Privileged EXEC mode to apply the commands in the script to the switch.

Syntax

`script apply scriptname`

- *scriptname* — Name of the script file to apply. (Range 1–31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example applies the *config.scr* script to the switch.

```
console#script apply config.scr
```

script delete

Use the **script delete** command in Privileged EXEC mode to delete a specified script.

Syntax

```
script delete {scriptname|a11}
```

- *scriptname* — Script name of the file being deleted. (Range 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example deletes all scripts from the switch.

```
console#script delete all
```

script list

Use the **script list** command in Privileged EXEC mode to list all scripts present on the switch as well as the remaining available space.

Syntax

`script list`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all scripts present on the switch.

```
console#script list
```

```
Configuration Script Name Size (Bytes)
```

```
-----
```

```
0 configuration script(s) found.
```

```
2048 Kbytes free.
```

script show

Use the **script show** command in Privileged EXEC mode to display the contents of a script file.

Syntax

`script show scriptname`

- *scriptname* — Name of the script file to be displayed. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the contents of the script file *config.scr*.

```
console#script show config.scr
interface ethernet 1/g1
ip address 176.242.100.100 255.255.255.0
exit
```

script validate

Use the **script validate** command in Privileged EXEC mode to validate a script file by parsing each line in the script file. The validate option is intended for use as a tool in script development. Validation identifies potential problems though it may not identify all problems with a given script.

Syntax

script validate *scriptname*

- *scriptname* — Name of the script file being validated. (Range: 1-31 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example validates the contents of the script file *config.scr*.

```
console#script validate config.scr
```

show backup-config

Use the **show backup-config** command in Privileged EXEC mode to display the contents of the backup configuration file.

Syntax

```
show backup-config
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example shows backup-config data.

```
console#show backup-config
software version 1.1
hostname device
interface ethernet 1/g1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000
exit
```

```
interface ethernet 1/g2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
exit
```

show bootvar

Use the **show bootvar** command in User EXEC mode to display the active system image file that the device loads at startup.

Syntax

```
show bootvar [unit]
```

- *unit* —Unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the active system image file that the device loads at startup.

```
console>show bootvar
```

```
Image Descriptions
```

```
image1 : default image
```

```
image2 :
```


Images currently available on Flash

unit	image1	image2	current-
active	next-active		

1	0.31.0.0	0.31.0.0	image2
image2			

show dir

Use the **show dir** command to list all the files available on the flash file system (TrueFlashFileSystem). The user can view the file names, and the size of each file.

Syntax Description

show dir

Default Configuration

This command has no default configuration

Command Mode

Privileged EXEC

User Guidelines

No specific guidelines.

Example

console#show dir

File name	Size (in bytes)
-----------	-----------------

image1	6351288
image2	6363424
fastpath.cfg	321894

show running-config

Use the **show running-config** command in Privileged EXEC mode to display the contents of the currently running configuration file. The command only displays the configurations that are non-default.



NOTE: All non-default configurations for the Captve Portal branding images and encoded Unicode are not displayed via the standard **show running-config** command. If desired, you can view this data in the script files or by using the **all** mode for the **show running-config** command. In addition, please note that this non-readable data is contained and displayed at the end of the script files.

Syntax

show running-config [*all* | *scriptname*]

- *all*—To display or capture the commands with settings and configuration that are equal to the default value, include the *all* option.
- *scriptname*—If the optional *scriptname* is provided, the output is redirected to a script file.



NOTE: If you issue the **show running-config** command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

show startup-config

Use the **show startup-config** command in Privileged EXEC mode to display the startup configuration file contents.

Syntax

show startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the contents of the startup-config file.

```
console#show startup-config
```

```
1 : !Current Configuration:
```

```
2 : !System Description "PowerConnect M8024, 1.0.0.0,  
VxWorks6.5"
```

```
3 : !System Software Version 1.0.0.0
```

```
4 : !
```

```
5 : configure
```

```
6 : vlan database
```

```
7 : vlan 3,1000-1001
```

```
8 : exit
```

```
9 : stack
```

```
10 : member 1 1
```

```
11 : exit
12 : ip address dhcp
13 : ip address vlan 1001
14 : interface vlan 3
15 : routing
16 : exit
17 : username "lvl7" password
fb3604df5a109405b2d79ecb06c47ab5 level 15 encrypted
18 : !
19 : interface ethernet 1/g17
20 : switchport mode general
21 : switchport general pvid 1001
22 : no switchport general acceptable-frame-type
tagged-only
23 : switchport general allowed vlan add 1000-1001
24 : switchport general allowed vlan remove 1
25 : exit
26 : !
27 : interface ethernet 1/xg3
28 : channel-group 1 mode auto
29 : exit
30 : !
31 : interface ethernet 1/xg4
32 : channel-group 1 mode auto
33 : exit
34 : snmp-server community public rw
35 : exit
```

update bootcode

Use the **update bootcode** command in Privileged EXEC mode to update the bootcode on one or more switches. For each switch, the bootcode is extracted from the active image and programmed to flash.

Syntax

update bootcode [*unit*]

- *unit*—Unit number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If *unit* is not specified, all units are updated.

Example

The following example updates the bootcode on unit 2.

```
console#update bootcode 2
```


Denial of Service Commands

This chapter explains the following commands:

- `dos-control firstfrag`
- `dos-control icmp`
- `dos-control l4port`
- `dos-control sipdip`
- `dos-control tcpflag`
- `dos-control tcpfrag`
- `ip icmp echo-reply`
- `ip icmp error-interval`
- `ip unreachable`
- `ip redirects`
- `ipv6 icmp error-interval`
- `ipv6 unreachable`
- `show dos-control`

dos-control firstfrag

Use the **dos-control firstfrag** command in Global Configuration mode to enable Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller than the configured value, the packets are dropped.

Syntax

dos-control firstfrag [*size*]

no dos-control firstfrag

- *size*—TCP header size. (Range: 0-255). The default TCP header size is 20. ICMP packet size is 512.

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example defines a minimum TCP header size of 20. Packets entering with a smaller header size are dropped.

```
console (config) #dos-control firstfrag 20
```

dos-control icmp

Use the **dos-control icmp** command in Global Configuration mode to enable Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets are dropped.

Syntax

dos-control icmp [*size*]

no dos-control icmp

- *size* — Maximum ICMP packet size. (Range: 0-1023). If size is unspecified, the value is 512.

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example activates the Maximum ICMP Packet Denial of Service protection with a maximum packet size of 1023.

```
console (config) #dos-control icmp 1023
```

dos-control l4port

Use the **dos-control l4port** command in Global Configuration mode to enable L4 Port Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets are dropped.

Syntax

dos-control l4port

no dos-control l4port

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example activates L4 Port Denial of Service protection.

```
console (config) #dos-control l4port
```

dos-control sipdip

Use the **dos-control sipdip** command in Global Configuration mode to enable Source IP Address = Destination IP Address (SIP=DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP=DIP, the packets is dropped if the mode is enabled.

Syntax

dos-control sipdip

no dos-control sipdip

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example activates SIP=DIP Denial of Service protection.

```
console (config) #dos-control sipdip
```

dos-control tcpflag

Use the **dos-control tcpflag** command in Global Configuration mode to enable TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024, having TCP Control Flags set to 0 and TCP Sequence Number set to 0, having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0, or having TCP Flags SYN and FIN both set, the packets are dropped.

Syntax

dos-control tcpflag

no dos-control tcpflag

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example activates TCP Flag Denial of Service protections.

```
console (config) #dos-control tcpflag
```

dos-control tcpfrag

Use the **dos-control tcpfrag** command in Global Configuration mode to enable TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP Fragment Offset equal to one (1), the packets are dropped.

Syntax

dos-control tcpfrag

no dos-control tcpfrag

Default Configuration

Denial of Service is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example activates TCP Fragment Denial of Service protection.

```
console (config) #dos-control tcpfrag
```

ip icmp echo-reply

Use the **ip icmp echo-reply** command to enable or disable the generation of ICMP Echo Reply messages. Use the “no” form of this command to prevent the generation of ICMP Echo Replies.

Syntax

ip icmp echo-reply

no ip icmp echo-reply

Default Configuration

ICMP Echo Reply messages are enabled by default.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ip icmp echo-reply
```

ip icmp error-interval

Use the **ip icmp error-interval** command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket with two configurable parameters: Burst-size and burst-interval.

To disable ICMP rate limiting, set burst-interval to zero. Use the “no” form of this command to return burst-interval and burst-size to their default values.

Syntax

ip icmp error-interval *burst-interval* [*burst-size*]

no ip icmp error-interval

- *burst-interval*— How often the token bucket is initialized (Range: 0–2147483647 milliseconds).
- *burst-size*— The maximum number of messages that can be sent during a burst interval (Range: 1–200).

Default Configuration

Rate limiting is enabled by default.

The default burst-interval is 1000 milliseconds.

The default burst-size is 100 messages.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command

Example

```
console(config)#ip icmp error-interval 1000 20
```

ip unreachable

Use the **ip unreachable** command to enable the generation of ICMP Destination Unreachable messages. Use the “no” form of this command to prevent the generation of ICMP Destination Unreachable messages.

Syntax

ip unreachable

no ip unreachable

Default Configuration

ICMP Destination Unreachable messages are enabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan10)#ip icmp unreachable
```

ip redirects

Use the **ip redirects** command to enable the generation of ICMP Redirect messages. Use the “no” form of this command to prevent the sending of ICMP Redirect Messages. In global configuration mode, this command affects all interfaces. In interface configuration mode, it only affects that interface.

Syntax

ip redirects

no ip redirects

Default Configuration

ICMP Redirect messages are enabled by default.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan10)#ip redirects
```

ipv6 icmp error-interval

Use the **icmp error-interval** command to limit the rate at which ICMP error messages are sent. The rate limit is configured as a token bucket with two configurable parameters: Burst-size and burst interval. Use the “no” form of this command to return burst-interval and burst-size to their default values. To disable ICMP rate limiting, set burst-interval to zero.

Syntax

ipv6 icmp error-interval *burst-interval* [*burst-size*]

no ipv6 icmp error-interval

- *burst-interval* — How often the token bucket is initialized (Range: 0–2147483647 milliseconds).
- *burst-size* — The maximum number of messages that can be sent during a burst interval (Range: 1–200).

Default Configuration

Rate limiting is enabled by default.

The default burst-interval is 1000 milliseconds.

The default burst-size is 100 messages.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config)#ipv6 icmp error-interval 2000 20
```

ipv6 unreachable

Use the **ipv6 unreachable** command to enable the generation of ICMPv6 Destination Unreachable messages. Use the “no” form of this command to prevent the generation of ICMPv6 Destination Unreachable messages.

Syntax

ipv6 unreachable

no ipv6 unreachable

Default Configuration

ICMPv6 Destination Unreachable messages are enabled by default.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

```
console(config-if-vlan10)#ipv6 unreachable
```

show dos-control

Use the **show dos-control** command in Privileged EXEC mode to display Denial of Service configuration information.

Syntax

`show dos-control`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

The following example displays Denial of Service configuration information.

```
console#show dos-control
```

```
SIPDIP Mode.....Disable
First Fragment Mode.....Disable
Min TCP Hdr Size.....20
TCP Fragment Mode..... Disable
TCP Flag Mode.....Disable
L4 Port Mode.....Disable
ICMP Mode.....Disable
Max ICMP Pkt Size.....512
```


Line Commands

This chapter explains the following commands:

- `exec-timeout`
- `history`
- `history size`
- `line`
- `show line`
- `speed`

exec-timeout

Use the **exec-timeout** command in Line Configuration mode to set the interval that the system waits for user input before timeout. To restore the default setting, use the **no** form of this command.

Syntax

exec-timeout *minutes* [*seconds*]

no exec-timeout

- *minutes* — Integer that specifies the number of minutes. (Range: 0–65535)
- *seconds* — Additional time intervals in seconds. (Range: 0–59)

Default Configuration

The default configuration is 10 minutes.

Command Mode

Line Configuration mode

User Guidelines

To specify no timeout, enter the **exec-timeout 0** command.

Example

The following example configures the interval that the system waits until user input is detected to 20 minutes.

```
console(config)#line console
console(config-line)#exec-timeout 20
```

history

Use the **history** command in Line Configuration mode to enable the command history function. To disable the command history function, use the **no** form of this command.

Syntax

history

no history

Default Configuration

The default value for this command is *enabled*.

Command Mode

Line Interface mode

User Guidelines

This command has no user guidelines.

Example

The following example disables the command history function for the current terminal session.

```
console(config-line)# no history
```

history size

Use the **history size** command in Line Configuration mode to change the command history buffer size for a particular line. To reset the command history buffer size to the default setting, use the **no** form of this command.

Syntax

history size *number-of-commands*

no history size

- *number-of-commands* — Specifies the number of commands the system may record in its command history buffer. (Range: 0-216)

Default Configuration

The default command history buffer size is 10.

Command Mode

Line Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the command history buffer size to 20 commands for the current terminal session.

```
console(config-line)#history size 20
```

line

Use the **line** command in Global Configuration mode to identify a specific line for configuration and enter the line configuration command mode.

Syntax

line {console | telnet | ssh}

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Examples

The following example enters Line Configuration mode to configure Telnet.

```
console(config)#line telnet
```

```
console(config-line)#
```

show line

Use the **show line** command in User EXEC mode to display line parameters.

Syntax

```
show line [console | telnet | ssh]
```

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the line configuration.

```
console>show line
```

```
Console configuration:
```

```
Interactive timeout: Disabled
```

```
History: 10
```

```
Baudrate: 9600
```

```
Databits: 8
```

```
Parity: none
```

```
Stopbits: 1
```

Telnet configuration:

Interactive timeout: 10 minutes 10 seconds

History: 10

SSH configuration:

Interactive timeout: 10 minutes 10 seconds

History: 10

speed

Use the **speed** command in Line Configuration mode to set the line baud rate. Use the **no** form of the command to restore the default settings.

Syntax

speed {*bps*}

no speed

- *bps* — Baud rate in bits per second (bps). The options are 2400, 9600, 19200, 38400, 57600, and 115200.

Default Configuration

This default speed is 9600.

Command Mode

Line Interface (console) mode

User Guidelines

This configuration applies only to the current session.

Example

The following example configures the console baud rate to 9600.

```
console(config-line)#speed 9600
```


Management ACL Commands

This chapter explains the following commands:

- deny (management)
- management access-class
- management access-list
- permit (management)
- show management access-class
- show management access-list

deny (management)

Use the **deny** command in Management Access-List Configuration mode to set conditions for the management access list.

Syntax

deny [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]
[**service** *service*] [**priority** *priority*]

deny **ip-source** *ip-address* [**mask** *mask* | *prefix-length*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*] [**service** *service*] [**priority** *priority*]

- **ethernet** *interface-number* — A valid Ethernet-routed port number.
- **vlan** *vlan-id* — A valid VLAN number.
- **port-channel** *number* — A valid routed port-channel number.
- *ip-address* — Source IP address.
- **mask** *mask* — Specifies the network mask of the source IP address.
- **mask** *prefix-length* — Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- **service** *service* — Indicates service type. Can be one of the following: telnet, ssh, http, https, tftp, or snmp.
- **priority** *priority* — Priority for the rule. (Range: 1–64)

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with **ethernet**, **vlan**, and **port-channel** parameters are valid only if an IP address is defined on the appropriate interface. Ensure that each rule has a unique priority.

Example

The following example shows how all ports are denied in the access-list called *mlist*.

```
console(config)# management access-list mlist
console(config-macal)# deny
```

management access-class

Use the **management access-class** command in Global Configuration mode to restrict management connections. To disable restriction, use the **no** form of this command.

Syntax

management access-class {**console-only** | *name*}

no management access-class

- *name* — A valid access-list name. (Range: 1–32 characters)
- **console-only** — The switch can be managed only from the console.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures an access-list called *mlist* as the management access-list.

```
console(config)# management access-class mlist
```

management access-list

Use the **management access-list** command in Global Configuration mode to define an access list for management, and enter the access-list for configuration. Once in the access-list configuration mode, the denied or permitted access conditions are configured with the **deny** and **permit** commands. To remove an access list, use the **no** form of this command.

Syntax

management access-list *name*

no management access-list *name*

- *name* — The access list name. (Range: 1–32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command enters the access-list configuration mode, where the denied or permitted access conditions with the **deny** and **permit** commands must be defined.

If no match criteria are defined the default is **deny**.

If reentering to an access-list context, the new rules are entered at the end of the access-list.

Use the **management access-class** command to select the active access-list.

The active management list cannot be updated or removed.

Examples

The following example shows how to configure two management interfaces, Ethernet 1/g1 and Ethernet 2/g9.

```
console(config)#management access-list mlist
```

```

console(config-macal)# permit ethernet 1/g1 priority
<1-64>

console(config-macal)# permit ethernet 2/g9 priority
<1-64>

console(config-macal)# exit

console(config)#management access-class mlist

```

The following example shows how to configure all the interfaces to be management interfaces except for two interfaces, Ethernet 1/g1 and Ethernet 2/g9.

```

console(config)# management access-list mlist

console(config-macal)# deny ethernet 1/g1 priority
<1-64>

console(config-macal)# deny ethernet 2/g9 priority
<1-64>

console(config-macal)# permit priority <1-64>

console(config-macal)# exit

console(config) # management access-class mlist

```

permit (management)

Use the **permit** command in Management Access-List configuration mode to set conditions for the management access list.

Syntax

```

permit ip-source ip-address [mask mask | prefix-length] [ethernet interface-
number | vlan vlan-id | port-channel number] [service service] [priority
priority-value]

```

```

permit {ethernet interface-number | vlan vlan-id | port-channel number}
[service service] [priority priority-value]

```

```

permit service service [priority priority-value]

```

```

permit priority priority-value

```

- *ethernet interface-number* — A valid routed port number.

- **vlan** *vlan-id* — A valid VLAN number.
- **port-channel** *number* — A valid port channel number.
- **ip-address** — Source IP address.
- **mask** *mask* — Specifies the network mask of the source IP address.
- **mask** *prefix-length* — Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- **service** *service* — Indicates service type. Can be one of the following: telnet, ssh, http, https, tftp, or snmp.
- **priority** *priority-value* — Priority for the rule. (Range: 1 – 64)

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

User Guidelines

Rules with **ethernet**, **vlan**, and **port-channel** parameters are valid only if an IP address is defined on the appropriate interface. Ensure that each rule has a unique priority.

Examples

The following example shows how to configure two management interfaces, Ethernet 1/g1 and Ethernet 2/g9.

```
console(config)#management access-list mlist
console(config-macal)# permit ethernet 1/g1 priority
<1-64>
console(config-macal)# permit ethernet 2/g9 priority
<1-64>
console(config-macal)# exit
console(config)# management access-class mlist
```

The following example shows how to configure all the interfaces to be management interfaces except for two interfaces, Ethernet 1/g1 and Ethernet 2/g9.

```
console(config)# management access-list mlist
console(config-macal)# deny ethernet 1/g1 priority
<1-64>
console(config-macal)# deny ethernet 2/g9 priority
<1-64>
console(config-macal)# permit priority <1-64>
console(config-macal)# exit
console(config)# management access-class mlist
```

show management access-class

Use the **show management access-class** command in Privileged EXEC mode to display information about the active management access list.

Syntax

show management access-class

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the management access-list information.

```
console# show management access-class
```

Management access-class is enabled, using access list
mlist

show management access-list

Use the **show management access-list** command in Privileged EXEC mode to display management access-lists.

Syntax

show management access-list [*name*]

- *name* — A valid access list name. (Range: 1–32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the active management access-list.

```
console# show management access-list
mlist
-----
permit priority 1 ethernet 1/g1
permit priority 2 ethernet 2/g1
! (Note: all other access implicitly denied)
```


Password Management Commands

This chapter explains the following commands:

- `passwords aging`
- `passwords history`
- `passwords lock-out`
- `passwords min-length`
- `show passwords configuration`

passwords aging

Use the **passwords aging** command in Global Configuration mode to implement expiration date on the passwords. The user is required to change the passwords when they expire.

Use the **no** form of this command to disable the aging function.

Syntax

passwords aging *age*

no passwords aging

- *age* — Time for the expiration of the password. (Range: 1-365 days)

Default Configuration

Password aging is disabled.

Command Mode

Global Configuration mode

User Guidelines

The passwords aging feature functions only if the switch clock is synchronized to an SNTP server. See “Clock Commands” on page 1083 for additional information.

Example

The following example sets the password age limit to 100 days.

```
console(config)#passwords aging 100
```

passwords history

As administrator, use the **passwords history** command in Global Configuration mode to set the number of previous passwords that are stored. This setting ensures that users do not reuse their passwords often.

Use the **no** form of this command to disable the password history function.

Syntax

`passwords history historylength`

`no passwords history`

- *historylength* — Number of previous passwords to be maintained in the history. (Range: 0–10.)

Default Configuration

No password history is maintained.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the number of previous passwords remembered by the system at 10.

```
console (config) #passwords history 10
```

passwords lock-out

As the administrator, use the **passwords lock-out** command in Global Configuration mode to strengthen the security of the switch by enabling the user lockout feature. When a lockout count is configured, a user who is logging in must enter the correct password within that count. Otherwise that user will be locked out from further switch access. Only an administrator with an access level of 15 can reactivate that user.

Use the **no** form of this command to disable the lockout feature.

Syntax

`passwords lock-out attempts`

`no passwords lock-out`

- *attempts* — Number of attempts the user is allowed to enter a correct password. (Range: 1-5)

Default Configuration

The user lockout feature is disabled.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

The following example sets the number of user attempts before lockout at 2.

```
console(config)#passwords lock-out 2
```

passwords min-length

Use the **passwords min-length** command in Global Configuration mode to configure the minimum length required for passwords in the local database. Use the **no** version of this command to disable any minimum password length limitation. If the password length requirement is disabled, users can be created with no password. In other words, when you issue the **no passwords min-length** command, the minimum password length is zero.

Syntax

passwords min-length *length*

no passwords min-length

- *length* — The minimum length of the password (Range: 8–64 characters)

Default Configuration

By default, the minimum password length is 8 characters.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the minimum password length to 12 characters.

```
console (config) #passwords min-length 12
```

show passwords configuration

Use the **show passwords configuration** command in Privileged EXEC mode to show the parameters for password configuration.

Syntax

```
show passwords configuration
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the command output.

```
console#show passwords configuration
```

```
passwords configuration:
```

```
Minimum password length           : disabled
```

```
Minimum password length value    : -
```

```
Password History                   : enabled
```

```
Password History length          : 8
```

aging	: enabled
aging value	: 30 days
User lockout	: enabled
User lockout attempts	: 3

PHY Diagnostics Commands

This chapter explains the following commands:

- `show copper-ports cable-length`
- `show copper-ports tdr`
- `show fiber-ports optical-transceiver`
- `test copper-port tdr`

show copper-ports cable-length

Use the **show copper-ports cable-length** command in Privileged EXEC mode to display the estimated copper cable length attached to a port.

Syntax

show copper-ports cable-length [*interface*]

- *interface* — A valid Ethernet port. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The port must be active and working in a 100M or 1000M mode.

Example

The following example displays the estimated copper cable length attached to all ports.

```
console#show copper-ports cable-length
```

Port	Length [meters]
-----	-----
1/g1	<50
1/g2	Copper not active
1/g3	110-140
1/g4	Fiber

show copper-ports tdr

Use the **show copper-ports tdr** command in Privileged EXEC mode to display the last Time Domain Reflectometry (TDR) tests on specified ports.

Syntax

show copper-ports tdr [*interface*]

- interface* — A valid Ethernet port. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The copper-related commands do not apply to the stacking, CX-4, or 10GBaseT ports associated with these plug-in modules.

The maximum length of the cable for the Time Domain Reflectometry (TDR) test is 120 meters.

Example

The following example displays the last TDR tests on all ports.

```
console#show copper-ports tdr
```

Port	Result	Length [meters]	Date
----	-----	-----	-----
1/g1	OK		
1/g2	Short	50	13:32:00 23 July 2004
1/g3	Test has not been preformed		
1/g4	Open	128	13:32:08 23 July 2004
1/g5	Fiber	-	-

show fiber-ports optical-transceiver

Use the `show fiber-ports optical-transceiver` command in Privileged EXEC mode to display the optical transceiver diagnostics.

Syntax

`show fiber-ports optical-transceiver` [*interface*]

- interface* — A valid Ethernet port. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The `show fiber ports` command is only applicable to the SFP combo ports and XFP ports (not the ports on the SFP+ plug-in module).

Examples

The following examples display the optical transceiver diagnostics.

```
console#show fiber-ports optical-transceiver
```

Port	Temp	Voltage	Current	Output Power	Input Power	TX Fault	LOS
1/g3	w	OK	E	OK	OK	OK	OK
1/g4	OK	OK	OK	OK	OK	E	OK
1/g1	Copper						

Temp - Internally measured transceiver temperature
Voltage - Internally measured supply voltage
Current - Measured TX bias current
Output Power - Measured TX output power in milliWatts
Input Power - Measured RX received power in milliWatts
TX Fault - Transmitter fault
LOS - Loss of signal

test copper-port tdr

Use the **test copper-port tdr** command in Privileged EXEC mode to diagnose with Time Domain Reflectometry (TDR) technology the quality and characteristics of a copper cable attached to a port.

Syntax

test copper-port tdr *interface*

- *interface* — A valid Ethernet port. The full syntax is *unit/port*.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines.

During the test shut down the port under test unless it is a combo port with an active fiber port.



NOTE: The maximum distance VCT can function is 120 meters.

Examples

The following example results in a report on the cable attached to port 1/g3.

```
console#test copper-port tdr 1/g3
```

```
Cable is open at 64 meters
```

The following example results in a failure to report on the cable attached to port 2/g3.

```
console#test copper-port tdr 2/g3
```

```
Can't perform the test on fiber ports
```


Power Over Ethernet Commands

This chapter explains the following commands:

- power inline
- power inline legacy
- power inline powered-device
- power inline priority
- power inline traps
- power inline usage-threshold
- show poe-firmware-version
- show power inline
- show power inline ethernet

power inline

The **power inline** command enables/disables the ability of the port to deliver power.

Syntax Description

power inline {auto | never}

no power inline

- **auto** — Enables the device discovery protocol and, if found, supplies power to the device.
- **never** — Disables the device discovery protocol and stops supplying power to the device.

Command Mode

Interface Configuration (Ethernet).

Usage Guidelines

No specific guidelines.

Default Value

auto

Examples

```
console(config)#interface ethernet 1/g1
```

```
console(config-if-1/g1)# power inline auto
```

power inline legacy

The **power inline legacy** command enables/disables the ability of the switch to support legacy Ethernet powered devices.

Syntax Description

power inline legacy

no power inline legacy

Parameter Ranges

Not applicable

Command Mode

Global Configuration.

Usage Guidelines

No specific guidelines.

Default Value

Legacy Support is disabled by default.

Examples

```
console(config)# power inline legacy
console(config)# no power inline legacy
```

power inline powered-device

The **power inline powered-device** Interface Configuration (Ethernet) mode command adds a comment or description of the powered device type to enable the user to remember what is attached to the interface. To remove the description, use the **no** form of this command.

Syntax Description

power inline powered-device *<pd-type>*

no power inline powered-device

- *pd-type* — Specifies the type of powered device attached to the interface. (Range: 1–24 characters)

Command Mode

Interface Configuration (Ethernet).

Usage Guidelines

No specific guidelines.

Examples

```
console(config)#interface ethernet 1/g1  
console(config-if-1/g1)# power inline powered-device  
IP-phone
```

power inline priority

The **power inline priority** command configures the port priority level, for the delivery of power to an attached device. The switch may not be able to supply power to all connected devices, so the port priority is used to determine which ports will supply power if adequate power capacity is not available for all enabled ports. For ports that have the same priority level, the lower-numbered port has higher priority.

For a system delivering peak power to a certain number of devices, if a new device is attached on a high-priority port, power will be shut down to a device on a low-priority port, and the new device will get powered up.

Syntax Description

power inline priority {critical | high | low}
no power inline priority

Command Mode

Interface Configuration (Ethernet).

Usage Guidelines

No specific guidelines.

Default Value

Low

Examples

```
console(config)#interface ethernet 1/g1  
console(config-if-1/g1)# power inline priority high
```


power inline traps

The **power inline traps** command enables inline power traps. To disable inline power traps, use the no form of this command.

Syntax Description

power inline traps *enable*

no power inline traps *enable*

- *enable* — Enables traps on the specified unit.

Command Mode

Global Configuration.

Usage Guidelines

No specific guidelines.

Default Value

disable

Examples

```
console(config)# power inline traps enable
```

power inline usage-threshold

The **power inline usage-threshold** command configures the system power usage threshold level at which a trap is generated. The threshold is configured as a percentage of the total available system power. As specified in the *Serial Communication Manual for PD63000* from PowerDSine, 06-0032-056 UG-PD63000 Serial Communication Protocol v5 2, Section 4.5.8, the power limit beyond which lower priority ports are disconnected has the configurable range from 37W to 806W. The maximum available system power for the 6224P and 6248P are 370W and 350W respectively. 37W is approximately 11 percent of these values. Thus, the minimum value of the usage-threshold can be configured as 11.

Syntax Description

power inline usage-threshold *<threshold>*

no power inline usage-threshold

- *threshold* — Power threshold at which trap is generated.

Parameter Ranges

<threshold> — 11–99 %

Command Mode

Global Configuration.

Usage Guidelines

No specific guidelines.

Default Value

95 %

Examples

```
console(config)# power inline usage-threshold 90
```

show poe-firmware-version

The `show poe-firmware-version` command displays the version of the PoE controller firmware present on the switch file system.

Syntax Description

show poe-firmware-version

Command Mode

Privileged EXEC.

Usage Guidelines

No specific guidelines.

Examples

```
console#show poe-firmware-version  
image version.....501_4
```

show power inline

The `show power inline` command displays the total available power, the total power consumed in the system, and the globally set usage threshold.

Syntax Description

`show power inline`

Parameter Ranges

None.

Command Mode

Privileged EXEC.

Usage Guidelines

No specific guidelines.

Example

```
console#show power inline  
Unit Status  
  
Unit1  
Power: On  
Nominal Power: 150 watt  
Consumed Power:120 watts (80%)  
  
Unit2
```

Power:On

Nominal Power:150 watt

Consumed Power:120 watts (80%)

Global Configuration

Usage Threshold:95%

Traps:Enabled

Port Configuration

Port	Powered	Device	State	Priority	Status	Classification
[w]						

-						

1/g1	IP Phone	Model	AAuto	High	On	0.44 - 12.95
------	----------	-------	-------	------	----	--------------

1/g2	Wireless AP	Model	Auto	Low	On	0.44 - 3.84
------	-------------	-------	------	-----	----	-------------

show power inline ethernet

The **show power inline ethernet** command displays the inline power summary for the interface.

Syntax Description

show power inline ethernet *<interface>*

- *interface* — A valid slot/port in the system.

Command Mode

Privileged EXEC.

Usage Guidelines

No specific guidelines.

Examples:

```
console#show power inline ethernet 1/g13
```

Port	Powered	Device	State	Priority	Status
Class [W]		Power [mW]			

--					
1/g13			auto	Low	On
3.84 - 6.49		5000			
Overload Counter.....					0
Short Counter.....					0
Denied Counter.....					0
Absent Counter.....					0
Invalid Signature Counter.....					0

RMON Commands

This chapter explains the following commands:

- rmon alarm
- rmon collection history
- rmon event
- show rmon alarm
- show rmon alarm-table
- show rmon collection history
- show rmon events
- show rmon history
- show rmon log
- show rmon statistics

rmon alarm

Use the **rmon alarm** command in Global Configuration mode to configure alarm conditions. To remove an alarm, use the **no** form of this command. Also see the related **show rmon alarm** command.

Syntax

rmon alarm *index variable interval rthreshold fthreshold revent fevent* [*type*] [*startup direction*] [*owner name*]

no rmon alarm *index*

- *index* — The alarm index. (Range: 1–65535)
- *variable* — A fully qualified SNMP object identifier that resolves to a particular instance of an MIB object.
- *interval* — The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. (Range: 1–4294967295)
- *rthreshold* — Rising Threshold. (Range: 0–4294967295)
- *fthreshold* — Falling Threshold. (Range: 0–4294967295)
- *revent* — The index of the Event that is used when a rising threshold is crossed. (Range: 1- 65535)
- *fevent* — The Event index used when a falling threshold is crossed. (Range: 1- 65535)
- *type type* — The sampling method for the selected variable and calculating the value to be compared against the thresholds. If the method is **absolute**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value at the last sample is subtracted from the current value, and the difference compared with the thresholds.
- *startup direction* — The alarm that may be sent when this entry is first set to valid. If the first sample (after this entry becomes valid) is greater than or equal to the *rthreshold*, and *direction* is equal to **rising** or **rising-falling**, then a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to the *fthreshold*, and *direction* is equal to **falling** or **rising-falling**, then a single falling alarm is generated.
- *owner name* — Enter a name that specifies who configured this alarm. If unspecified, the name is an empty string.

Default Configuration

The following parameters have the following default values:

- **type** *type* — If unspecified, the type is **absolute**.
- **startup** *direction* — If unspecified, the startup direction is **rising-falling**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the following alarm conditions:

- Alarm index — 1
- Variable identifier — 1.3.6.1.2.1.2.2.1.10.5
- Sample interval — 10 seconds
- Rising threshold — 500000
- Falling threshold — 10
- Rising threshold event index — 1
- Falling threshold event index — 1

```
console(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.1.10.5 10  
50000 10 1 1
```

rmon collection history

Use the **rmon collection history** command in Interface Configuration mode to enable a Remote Monitoring (RMON) MIB history statistics group on an interface. To remove a specified RMON history statistics group, use the **no** form of this command. Also see the **show rmon collection history** command.

Syntax

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*]
[**interval** *seconds*]

no rmon collection history *index*

- *index* — The requested statistics index group. (Range: 1–65535)
- **owner** *ownername* — Records the RMON statistics group owner name. If unspecified, the name is an empty string.
- **buckets** *bucket-number* — A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range: 1 - 65535)
- **interval** *seconds* — The number of seconds in each polling cycle. If unspecified, defaults to 1800. (Range: 1–3600)

Default Configuration

The **buckets** configuration is 50. The **interval** configuration is 1800 seconds.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode.

User Guidelines

This command cannot be executed on multiple ports using the **interface** range **ethernet** command.

Example

The following example enables a Remote Monitoring (RMON) MIB history statistics group on port 1/g8 with the index number "1" and a polling interval period of 2400 seconds.

```
console(config)#interface ethernet 1/g8  
  
console(config-if-1/g8)#rmon collection history 1  
interval 2400
```

rmon event

Use the **rmon event** command in Global Configuration mode to configure an event. To remove an event, use the **no** form of this command. Also see the **show rmon events** command.

Syntax

rmon event *index type* [*community text*] [*description text*] [*owner name*]

no rmon event *index*

- *index* — The event index. (Range: 1–65535)
- *type* — The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
- *community text* — If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string. (Range: 0-127 characters)
- *description text* — A comment describing this event. (Range 0-127 characters)
- *owner name* — Enter a name that specifies who configured this event. If unspecified, the name is an empty string.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures an event with the trap index of 10.

```
console(config)#rmon event 10 log
```

show rmon alarm

Use the **show rmon alarm** command in User EXEC mode to display alarm configuration. Also see the **rmon alarm** command.

Syntax

show rmon alarm *number*

- *number* — Alarm index. (Range: 1–65535)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays RMON 1 alarms.

```
console> show rmon alarm 1
Alarm 1
-----
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
```

Falling Event: 1

Owner: CLI

The following table describes the significant fields shown in the display:

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	The statistic value during the last sampling period. For example, if the sample type is delta, this value is the difference between the samples at the beginning and end of the period. If the sample type is absolute, this value is the sampled value at the end of the period.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is absolute , the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is delta , the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Startup Alarm	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.
Rising Threshold	A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.
Owner	The entity that configured this entry.

show rmon alarm-table

Use the `show rmon alarm-table` command in User EXEC mode to display the alarms summary table.

Syntax

`show rmon alarm-table`

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the alarms summary table:

```
console> show rmon alarm-table
```

Index	OID	Owner
-----	-----	-----
1	1.3.6.1.2.1.2.2.1.10.1	CLI
2	1.3.6.1.2.1.2.2.1.10.1	Manager
3	1.3.6.1.2.1.2.2.1.10.9	CLI

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

show rmon collection history

Use the `show rmon collection history` command in User EXEC mode to display the requested group of statistics. Also see the `rmon collection history` command.

Syntax

`show rmon collection history [ethernet interface | port-channel port-channel-number]`

- *interface* — Valid Ethernet port. The full syntax is *unit /port*.
- *port-channel-number* — Valid trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all RMON group statistics.

```
console> show rmon collection history
```

Index	Interface	Interval	Requested Samples	Granted Samples	Owner

1	1/g1	30	50	50	CLI
2	1/g1	1800	50	50	Manager

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface.
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

show rmon events

Use the `show rmon events` command in User EXEC mode to display the RMON event table. Also see the `rmon event` command.

Syntax

`show rmon events`

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the RMON event table.

```
console> show rmon events
```

Index	Description	Type	Community	Owner	Last time sent
-----	-----	----	-----	-----	-----
1	Errors	Log	CLI		Jan 18 2005 23:58:17
2	High Broadcast	Log-Trap	switch	Manager	Jan 18 2005 23:59:48

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	The type of notification that the device generates about this event. Can have the following values: none , log , trap , log-trap . In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

show rmon history

Use the **show rmon history** command in User EXEC mode to display RMON Ethernet Statistics history. Also see the **rmon history** command.

Syntax

show rmon history *index* [**throughput** | **errors** | **other**] [**period** *seconds*]

- *index* — The requested set of samples. (Range: 1–65535)
- **throughput** — Displays throughput counters.
- **errors** — Displays error counters.
- **other** — Displays drop and collision counters.
- **period** *seconds* — Specifies the requested period time to display. (Range: 0–2147483647)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Examples

The following example displays RMON Ethernet Statistics history for "throughput" on index number 1.

```
console> show rmon history 1 throughput
Sample Set: 1 Owner: CLI
Interface: 1/g1 interval: 1800
Requested samples: 50      Granted samples: 50
Maximum table size: 270
```

Time		Octets	Packets	Broadcast	Multicast	%
09-Mar-2005	18:29:32	303595962	357568	3289	7287	19
09-Mar-2005	18:29:42	287696304	275686	2789	5878	20

The following example displays RMON Ethernet Statistics history for errors on index number 1.

```
console> show rmon history 1 errors
Sample Set: 1      Owner: Me
Interface: 1/g1    interval: 1800
Requested samples: 50      Granted samples: 50
Maximum table size: 500 (800 after reset)
```

Time		CRC Align	Undersize	Oversize	Fragments	Jabbers
09-Mar-2005	18:29:32	1	1	0	49	0
09-Mar-2005	18:29:42	1	1	0	27	0

The following example displays RMON Ethernet Statistics history for "other" on index number 1.

```
console> show rmon history 1 other
Sample Set: 1                               Owner: Me
Interface:  1/g1 Interval: 1800
Requested samples: 50                       Granted samples: 50
Maximum table size: 270

Time                               Dropped      Collisions
-----
10-Mar-2005  22:06:00              3              0
10-Mar-2005  22:06:20              3              0
```

The following table describes the significant fields shown in the display:

Field	Description
Time	Date and Time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the Broadcast address.
Multicast	The number of good packets received during this sampling interval that were directed to a Multicast address. This number does not include packets addressed to the Broadcast address.
%	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Field	Description
Undersize	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runs (which are normal occurrences due to collisions) and noise hits.
Jabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped. It is just the number of times this condition has been detected.
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

show rmon log

Use the `show rmon log` command in User EXEC mode to display the RMON logging table.

Syntax

`show rmon log [event]`

- *event* — Event index. (Range: 1–65535)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display the RMON logging table.

```
console> show rmon log
```

```
Maximum table size: 100
```

Event Description		Time	
-----		-----	
1	Errors	Jan 18 2005	23:48:19
1	Errors	Jan 18 2005	23:58:17
2	High Broadcast	Jan 18 2005	23:59:48

```
console> show rmon log
```

```
Maximum table size: 100 (100 after reset)
```

Event	Description	Time
1	Errors	Jan 18 2005 23:48:19
1	Errors	Jan 18 2005 23:58:17
2	High Broadcast	Jan 18 2005 23:59:48

The following table describes the significant fields shown in the display:

Field	Description
Event	An index that uniquely identifies the event.
Description	A comment describing this event.
Time	The time this entry was created.

show rmon statistics

Use the **show rmon statistics** command in User EXEC mode to display RMON Ethernet Statistics.

Syntax

show rmon statistics {*ethernet interface* | *port-channel port-channel-number*}

- *interface* — Valid Ethernet unit/port.
- *port-channel-number* — Valid port-channel trunk index.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays RMON Ethernet Statistics for port 1/g1.

```
console> show rmon statistics ethernet 1/g1

Port 1/g1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0

128 to 255 Octets: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

The following table describes the significant fields shown in the display:

Field	Description
Dropped	The total number of events in which packets are dropped by the probe due to lack of resources. This number is not always the number of packets dropped; it is the number of times this condition has been detected.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, Broadcast packets, and Multicast packets) received.

Field	Description
Broadcast	The total number of good packets received and directed to the Broadcast address. This does not include Multicast packets.
Multicast	The total number of good packets received and directed to a Multicast address. This number does not include packets directed to the Broadcast address.
CRC Align Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize Pkts	The total number of packets received less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	The total number of packets received less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	The total number of packets received longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Field	Description
128 to 255 Octets	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to 1518 Octets	The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Serviceability Tracing Packet Commands

This chapter explains the following commands:

- debug arp
- debug auto-voip
- debug clear
- debug console
- debug dot1x
- debug igmpsnooping
- debug ip acl
- debug ip dvmrp
- debug ip igmp
- debug ip mcache
- debug ip pimdm
- debug ip pimsm
- debug ip vrrp
- debug ipv6 mcache
- debug ipv6 mld
- debug ipv6 pimdm
- debug ipv6 pimsm
- debug isdp
- debug lacp
- debug mldsnooping
- debug ospf
- debug ospfv3
- debug ping

- debug rip
- debug sflow
- debug spanning-tree
- show debugging



NOTE: Debug commands are not persistent across resets.

debug arp

Use the **debug arp** command to enable tracing of ARP packets. Use the “no” form of this command to disable tracing of ARP packets.

Syntax

debug arp

no debug arp

Default Configuration

ARP packet tracing is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug arp
```

debug auto-voip

Use the **debug auto-voip** command to enable Auto VOIP debug messages.

Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Use the “no” form of this command to disable Auto VOIP debug messages.

Syntax

debug auto-voip [H323 | SCCP | SIP]

no debug auto-voip [H323 | SCCP | SIP]

Default Configuration

Auto VOIP tracing is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug auto-voip
```

debug clear

Use the **debug clear** command to disable all debug traces.

Syntax

```
debug clear
```

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug clear
```

debug console

Use the **debug console** to enable the display of “debug” trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands

appears on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Syntax

`debug console`

Default Configuration

Display of debug traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug console
```

debug dot1x

Use the `debug dot1x` command to enable dot1x packet tracing. Use the “no” form of this command to disable dot1x packet tracing.

Syntax

`debug dot1x packet [receive | transmit]`
`no debug dot1x packet [receive | transmit]`

Default Configuration

Display of dot1x traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug dot1x packet
```

debug igmpsnooping

Use the **debug igmpsnooping** to enable tracing of IGMP Snooping packets transmitted and/or received by the switch. IGMP Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Syntax

```
debug igmpsnooping packet [receive | transmit]
```

```
no debug igmpsnooping packet [receive | transmit]
```

Default Configuration

Display of IGMP Snooping traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug igmpsnooping packet
```

debug ip acl

Use the **debug ip acl** command to enable debug of IP Protocol packets matching the ACL criteria. Use the “no” form of this command to disable IP ACL debugging.

Syntax

`debug ip acl acl`

`no debug ip acl acl`

- *acl* — The number of the IP ACL to debug.

Default Configuration

Display of IP ACL traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ip  acl 1
```

debug ip dvmrp

Use the `debug ip dvmrp` to trace DVMRP packet reception and transmission. The `receive` option traces only received DVMRP packets and the `transmit` option traces only transmitted DVMRP packets. When neither keyword is used in the command, all DVMRP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Syntax

`debug ip dvmrp packet [receive | transmit]`

`no debug ip dvmrp packet [receive | transmit]`

Default Configuration

Display of DVMRP traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ip  dvmrp packet
```

debug ip igmp

Use the **debug ip igmp** command to trace IGMP packet reception and transmission. The **receive** option traces only received IGMP packets and the **transmit** option traces only transmitted IGMP packets. When neither keyword is used in the command, then all IGMP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable IGMP traces.

Syntax

```
debug ip igmp packet [receive | transmit]
```

```
no debug ip igmp packet [receive | transmit]
```

Default Configuration

Display of IGMP traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ip igmp packet
```

debug ip mcache

Use the **debug ip mcache** command for tracing MDATA packet reception and transmission. The **receive** option traces only received data packets and the **transmit** option traces only transmitted data packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable MDATA tracing.

Syntax

```
debug ip mcache packet [receive | transmit]
```

```
no debug ip mcache packet [receive | transmit]
```

Default Configuration

Display of MDATA traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ip mcache packet
```

debug ip pimdm

Use the **debug ip pimdm** command to trace PIMDM packet reception and transmission. The **receive** option traces only received PIMDM packets and the **transmit** option traces only transmitted PIMDM packets. When neither keyword is used in the command, then all PIMDM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable PIMDM tracing.

Syntax

```
debug ip pimdm packet [receive | transmit]
no debug ip pimdm packet [receive | transmit]
```

Default Configuration

Display of PIMDM traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ip pimdm packet
```

debug ip pimsm

Use the **debug ip pimsm** command to trace PIMSM packet reception and transmission. The **receive** option traces only received PIMSM packets and the **transmit** option traces only transmitted PIMSM packets. When neither keyword is used in the command, then all PIMSM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable PIMSM tracing.

Syntax

```
debug ip pimsm packet [receive | transmit]
no debug ip pimsm packet [receive | transmit]
```

Default Configuration

Display of PIMSM traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ip pimsm packet
```

debug ip vrrp

Use the **debug ip vrrp** command to enable VRRP debug protocol messages. Use the “no” form of this command to disable VRRP debug protocol messages.

Syntax

```
debug ip vrrp
```

```
no debug ip vrrp
```

Default Configuration

Display of VRRP traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

```
console#debug ip vrrp
```

debug ipv6 mcache

Use the **debug ipv6 mcache** command to trace MDATAv6 packet reception and transmission. The **receive** option traces only received data packets and the **transmit** option traces only transmitted data packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Syntax

debug ipv6 mcache packet [receive | transmit]

no debug ipv6 mcache packet [receive | transmit]

Default Configuration

Display of MDATA traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

This command has no user guidelines.

Example

```
console#debug ipv6 mcache packet
```

debug ipv6 mld

Use the **debug ipv6 mld** command to trace MLD packet reception and transmission. The **receive** option traces only received MLD packets and the **transmit** option traces only transmitted MLD packets. When neither keyword is used in the command, then all MLD packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable MLD tracing.

Syntax

```
debug ipv6 mld packet [receive | transmit]  
no debug ipv6 mld packet [receive | transmit]
```

Default Configuration

Display of MLD traces is disabled by default.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ipv6 mld packet
```

debug ipv6 pimdm

Use the **debug ipv6 pimdm** command to trace PIMDMv6 packet reception and transmission. The **receive** option traces only received PIMDMv6 packets and the **transmit** option traces only transmitted PIMDMv6 packets. When neither keyword is used in the command, then all PIMDMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable PIMDMv6 tracing.

Syntax

```
debug ipv6 pimdm packet [receive | transmit]  
no debug ipv6 pimdm packet [receive | transmit]
```

Default Configuration

Display of PIMDMv6 traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ipv6 pimdm packet
```

debug ipv6 pimsm

Use the **debug ipv6 pimsm** command to trace PIMSMv6 packet reception and transmission. The **receive** option traces only received PIMSMv6 packets and the **transmit** option traces only transmitted PIMSMv6 packets. When neither keyword is used in the command, then all PIMSMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable PIMSMv6 tracing.

Syntax

```
debug ipv6 pimsm packet [receive | transmit]  
no debug ipv6 pimsm packet [receive | transmit]
```

Default Configuration

Display of PIMSMv6 traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ipv6 pimsm packet
```


debug isdp

Use the **debug isdp** command to trace ISDP packet reception and transmission. The **receive** option traces only received ISDP packets and the **transmit** option traces only transmitted ISDP packets. When neither keyword is used in the command, then all ISDP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable ISDP tracing.

Syntax

```
debug isdp packet [receive | transmit]
```

```
no debug isdp packet [receive | transmit]
```

Default Configuration

Display of ISDP traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug isdp packet
```

debug lacp

Use the **debug lacp** command to enable tracing of LACP packets received and transmitted by the switch. Use the “no” form of this command to disable tracing of LACP packets.

Syntax

```
debug lacp packet
```

```
no debug lacp packet
```

Default Configuration

Display of LACP traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug lacp packet
```

debug mldsnooping

Use the **debug mldsnooping** command to trace MLD snooping packet reception and transmission. The **receive** option traces only received MLD snooping packets and the **transmit** option traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable tracing of MLD Snooping packets.

Syntax

```
debug mldsnooping packet [receive | transmit]
```

```
no debug mldsnooping packet [receive | transmit]
```

Default Configuration

Display of MLD Snooping traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug mldsnooping
```

debug ospf

Use the **debug ospf** command to enable tracing of OSPF packets received and transmitted by the switch. Use the “no” form of this command to disable tracing of OSPF packets.

Syntax

```
debug ospf packet
```

```
no debug ospf packet
```

Default Configuration

Display of OSPF traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ospf packet
```

debug ospfv3

Use the **debug ospfv3** command to enable tracing of OSPFv3 packets received and transmitted by the switch. Use the “no” form of this command to disable tracing of OSPFv3 packets.

Syntax

```
debug ospfv3 packet  
no debug ospfv3 packet
```

Default Configuration

Display of OSPFv3 traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug ospfv3 packet
```

debug ping

Use the **debug ping** command to enable tracing of ICMP echo requests and responses. This command traces pings on the network port and on the routing interfaces. Use the “no” form of this command to disable tracing of ICMP echo requests and responses.

Syntax

```
debug ping packet  
no debug ping packet
```

Default Configuration

Display of ICMP echo traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

The following example displays.

```
console#debug ping packet
```

debug rip

Use the **debug rip** command to enable tracing of RIP requests and responses. Use the “no” form of this command to disable tracing of RIP requests and responses.

Syntax

```
debug rip packet
```

```
no debug rip packet
```

Default Configuration

Display of RIP traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug rip packet
```

debug sflow

Use the **debug sflow** command to enable sFlow debug packet trace. Use the “no” form of this command to disable sFlow packet tracing.

Syntax

`debug sflow packet`

`no debug sflow packet`

Default Configuration

Display of sFlow traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug sflow packet
```

debug spanning-tree

Use the **debug spanning-tree** command to trace spanning tree BPDU packet reception and transmission. The **receive** option traces only received spanning tree BPDUs and the **transmit** option traces only transmitted BPDUs. When neither keyword is used in the command, all spanning tree BPDU traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console. Use the “no” form of this command to disable tracing of spanning tree BPDUs.

Syntax

`debug spanning-tree bpdv [receive | transmit]`

`no debug spanning-tree bpdv [receive | transmit]`

Default Configuration

Display of spanning tree BPDU traces is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guidelines

There are no usage guidelines for this command.

Example

```
console#debug spanning-tree bpdu
```

show debugging

Use the `show debugging` command to display packet tracing configurations.

Syntax

```
show debugging
```

```
no show debugging
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

Usage Guidelines

Enabled packet tracing configurations are displayed.

Example

```
console #debug arp
```

```
Arp packet tracing enabled.
```

```
console #show debugging
```

```
Arp packet tracing enabled.
```


sFlow Commands

This chapter explains the following commands:

- sflow destination
- sflow polling
- sflow polling (Interface Mode)
- sflow sampling
- sflow sampling (Interface Mode)
- show sflow agent
- show sflow destination
- show sflow polling
- show sflow sampling

sflow destination

Use the **sflow destination** command to configure the sFlow collector parameters (owner string, receiver timeout, maxdatagram, ip address and port). Use the “no” form of this command to set receiver parameters to the default or remove a receiver.

Syntax

```
sflow rcvr_index destination {ip-address [port] | maxdatagram size | owner "owner_string" timeout rcvr_timeout}
```

```
no sflow receiver rcvr_index destination {ip-address | maxdatagram | owner}
```

- *rcvr_index*—The index of this sFlow Receiver (Range: 1–8).
- *ip-address*—The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent.
- *size*—The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. (Range: 200–9116 bytes).
- *owner_string*—The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The default is an empty string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller. (Range: 1–127 characters).
- *rcvr_timeout*—The time, in seconds, remaining before the sampler or poller is released and stops sending samples to the receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. (Range: 0–4294967295 seconds).
- *port*—The destination Layer4 UDP port for sFlow datagrams. (Range: 1–65535).

Default Configuration

No receivers are configured by default.

The default IP address is 0.0.0.0

The default maximum datagram size is 1400.

The default owner string is the empty string.

The default receiver timeout is 0.

The default port is 6343.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines

Example

```
console(config)#sflow 1 destination owner 1 timeout 2000
```

```
console(config)#sflow 1 destination maxdatagram 500
```

```
console(config)#sflow 1 destination 30.30.30.1 560
```

sflow polling

Use the **sflow polling** command to enable a new sflow poller instance for this data source if *rcvr_idx* is valid. Use the “no” form of this command to reset poller parameters to the defaults.

Syntax

sflow *rcvr-index* **polling** **ethernet** *interfaces* *poll-interval*

no sflow *rcvr-index* **polling** **ethernet** *interfaces*

- *rcvr-index* — The sFlow Receiver associated with the poller (Range: 1–8).

- *interfaces* — The list of interfaces to poll.
- *poll-interval* — The sFlow instance polling interval. A poll interval of 0 disables counter sampling. A value of *n* means once in *n* seconds a counter sample is generated. (Range: 0–86400).

Default Configuration

There are no pollers configured by default.

The default poll interval is 0.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config)#sflow 1 polling ethernet 1/g1-1/g10
200
```

sflow polling (Interface Mode)

Use the **sflow polling** command in Interface Mode to enable a new sflow poller instance for this data source if *rcvr_idx* is valid. Use the "no" form of this command to reset poller parameters to the defaults.

Syntax

sflow *rcvr-index* **polling** *poll-interval*

no sflow polling

- *rcvr-index* — The sFlow Receiver associated with the poller (Range: 1 - 8).
- *poll-interval* — The sFlow instance polling interval. A poll interval of 0 disables counter sampling. A value of *n* means once in *n* seconds a counter sample is generated. (Range: 0 - 86400).

Default Configuration

There are no pollers configured by default.

The default poll interval is 0.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/g2)#sflow 1 polling 6055
```

sflow sampling

Use the **sflow sampling** command to enable a new sflow sampler instance for this data source if `rcvr_idx` is valid. Use the “no” form of this command to reset sampler parameters to the default.

Syntax

sflow *rcvr-index* **sampling** **ethernet** *interfaces* *sampling-rate* [*size*]

no sflow *rcvr-index* **sampling** **ethernet** *interfaces*

- *rcvr-index*—The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. If no receiver is configured, then no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. (Range: 1–8).
- *interfaces* — The list of interfaces to poll.
- *sampling-rate*—The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A rate of 0 disables sampling. A value of *n* means that out of *n* incoming packets, 1 packet will be sampled. (Range: 1024–65536).
- *size*—The maximum number of bytes that should be copied from the sampler packet (Range: 20–256 bytes).

Default Configuration

There are no samplers configured by default.

The default sampling rate is 0.

The default maximum header size is 128.

Command Mode

Global Configuration mode.

User Guidelines

This command has no user guidelines.

Example

```
console(config)#sflow 1 sampling ethernet 1/g2 1500 50
```

sflow sampling (Interface Mode)

Use the **sflow sampling** command in Interface Mode to enable a new sflow sampler instance for this data source if *rcvr_idx* is valid. Use the "no" form of this command to reset sampler parameters to the default.

Syntax

sflow *rcvr-index* **sampling** *sampling-rate* [*size*]

no sflow *rcvr-index* **sampling**

- *rcvr-index* — The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. If no receiver is configured, then no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. (Range: 1 - 8).
- *sampling-rate* — The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A rate of 0 disables sampling. A value of n means that out of n incoming packets, 1 packet will be sampled. (Range: 1024 - 65536).
- *size* — The maximum number of bytes that should be copied from the sampler packet (Range: 20 - 256 bytes).

Default Configuration

There are no samplers configured by default.

The default sampling rate is 0.

The default maximum header size is 128.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command has no user guidelines.

Example

```
console(config-if-1/g15)#sflow 1 sampler 1500 50
```

show sflow agent

Use the `show sflow agent` command to display the sflow agent information.

Syntax

`show sflow agent`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

The following fields are displayed:

sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: MIB Version: 1.3, the version of this MIB. Organization: Dell Corp. Revision: 1.0
IP Address	The IP address associated with this agent.

Example

console#show sflow agent

```
sFlow Version..... 1.3;Dell
Corp.;10.23.18.28
IP Address..... 0.0.0.0
```

show sflow destination

Use the **show sflow destination** command to display all the configuration information related to the sFlow receivers.

Syntax

show sflow *rcvr-index* destination

- *rcvr index*—The index of the sFlow Receiver to display (Range: 1–8).

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

The following fields are displayed:

Receiver Index	The sFlow Receiver associated with the sampler/poller.
----------------	--

Owner String	The identity string for receiver, the entity making use of this sFlowRcvrTable entry.
Time Out	The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver.
Max Datagram Size	The maximum number of bytes that can be sent in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.

Example

```
console# show sflow 2 destination
```

Receiver Index	Owner String	Time out	Max Datagram Size	Port	IP Address
2		0	1400	6343	0.0.0.0

show sflow polling

Use the **show sflow polling** command to display the sFlow polling instances created on the switch.

Syntax

show sflow *rcvr-index* polling [*ethernet interfaces*]

- *rcvr-index* — The sFlow Receiver associated with the poller (Range: 1–8).
- *interfaces* — The list of interfaces to poll.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

The following fields are displayed:

Poller Data Source	The sFlowDataSource (unit/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver associated with this sFlow counter poller.
Poller Interval	The number of seconds between successive samples of the counters associated with this data source.

Example

```
console# show sflow 1 polling
```

Poller	Receiver	Poller
Data Source	Index	Interval
-----	-----	-----
1/g1	1	0

show sflow sampling

Use the `show sflow sampling` command to display the sFlow sampling instances created on the switch.

Syntax

`show sflow rcvr-index sampling [ethernet interfaces]`

- *rcvr-index* — The sFlow Receiver associated with the poller (Range: 1–8).
- *interfaces* — The list of interfaces on which data is sampled.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode.

User Guidelines

The following fields are displayed:

Sampler Data Source	The sFlowDataSource (unit/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver configured for this sFlow sampler.
Packet Sampling Rate	The statistical sampling rate for packet sampling from this source.
Max Header Size	The maximum number of bytes that should be copied from a sampled packet to form a flow sample.

Example

```
console# #show sflow 1 sampling
```

Sampler Data Source	Receiver Index	Packet Sampling Rate	Max Header Size
-----	-----	-----	-----
1/g1	1	0	128

SNMP Commands

This chapter explains the following commands:

- `show snmp`
- `show snmp engineID`
- `show snmp filters`
- `show snmp groups`
- `show snmp users`
- `show snmp views`
- `show trapflags`
- `snmp-server community`
- `snmp-server community-group`
- `snmp-server contact`
- `snmp-server enable traps`
- `snmp-server enable traps authentication`
- `snmp-server engineID local`
- `snmp-server filter`
- `snmp-server group`
- `snmp-server host`
- `snmp-server location`
- `snmp-server user`
- `snmp-server view`
- `snmp-server v3-host`

show snmp

Use the `show snmp` command in Privileged EXEC mode to display the SNMP communications status.

Syntax

`show snmp`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the SNMP communications status.

```
Console # show snmp
```

Community-String	Community-Access	View name	IP address
-----	-----	-----	-----
public	read only	user-view	All
private	read write	Default	172.16.1.1
private	su	DefaultSuper	172.17.1.1

Community-String	Group name	IP address
-----	-----	-----
public	user-group	All

```
Traps are enabled.
```

```
Authentication trap is enabled.
```

```
Version 1,2 notifications
```

Target Address	Type	Community	Version	UDP Port	Filter name	TO Sec	Retries
-----	-----	-----	-----	----	-----	---	-----
192.122.173.42	Trap	public	=2	162	filt1	15	3
192.122.173.42	Inform	public	2	162	filt2	15	3

Version 3 notifications

Target Address	Type	Username	Security Level	UDP Port	Filter name	TO Sec	Retries
-----	-----	-----	-----	----	-----	---	-----
192.122.173.42	Inform	Bob	Priv	162	filt31	15	3

System Contact: Robert

System Location: Marketing

show snmp engineID

Use the `show snmp engineID` command in Privileged EXEC mode to display the ID of the local Simple Network Management Protocol (SNMP) engine.

Syntax

`show snmp engineID`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the SNMP engine ID.

```
console# show snmp engineID
```

```
Local SNMP engineID: 08009009020C0B099C075878
```

show snmp filters

Use the `show snmp filters` command in Privileged EXEC mode to display the configuration of filters.

Syntax

`show snmp filters filtername`

- filtername* — Specifies the name of the filter. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display the configuration of filters with and without a filter name specification.

```
console # show snmp filters
```

Name	OID Tree	Type

-		
user-filter1	1.3.6.1.2.1.1	Included
user-filter1	1.3.6.1.2.1.1.7	Excluded
user-filter2	1.3.6.1.2.1.2.2.1.*.1	Included

```
console # show snmp filters user-filter1
```


Name	OID Tree	Type

-		
user-filter1	1.3.6.1.2.1.1	Included
user-filter1	1.3.6.1.2.1.1.7	Excluded

show snmp groups

Use the `show snmp groups` command in Privileged EXEC mode to display the configuration of groups.

Syntax

`show snmp groups [groupname]`

- *groupname* — Specifies the name of the group. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display the configuration of views.

```
console# show snmp groups
```

Name	Security		Views		
	Model	Level	Read	Write	Notify

user-group	V3	Auth-Priv	Default	" "	" "
managers-group	V3	NoAuth-priv	Default	Default	" "

```
managers-group      V3      NoAuth-priv  Default  " "      " "
```

```
console# show snmp groups user-group
```

Name	Security		Views		
	Model	Level	Read	Write	Notify
-----	-----	-----	-----	-----	-----
user-group	V3	Auth-Priv	Default	" "	" "

The following table contains field descriptions.

Field	Description
Name	Name of the group
Security Model	SNMP model in use (v1, v2 or v3)
Security Level	Authentication of a packet with encryption. Applicable only to SNMP Version 3 security model.
Views	<ul style="list-style-type: none">• Read—A string that is the name of the view that enables you only to view the contents of the agent. If unspecified, all the objects except the community-table and SNMPv3 user and access tables are available.• Write—A string that is the name of the view that enables you to enter data and manage the contents of the agent.• Notify—A string that is the name of the view that enables you to specify an inform or a trap.

show snmp users

Use the `show snmp users` Privileged EXEC command to display the configuration of users.

Syntax

`show snmp users` [*username*]

- *username* — Specifies the name of the user. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the configuration of users with the user name specified.

```
Console # show snmp users
```

Name	Group Name	Auth Priv		Remote Engine ID
		Meth	Meth	
-----	-----	-----	-----	-----
bob	user-group	MD5	DES	800002a20300fce3900106
john	user-group	SHA	DES	800002a20300fce3900106

```
Console # show snmp users bob
```

Name	Group Name	Auth Priv		Remote Engine ID
		Meth	Meth	
-----	-----	-----	-----	-----
bob	user-group	MD5	DES	800002a20300fce3900106

show snmp views

Use the `show snmp views` command in Privileged EXEC mode to display the configuration of views.

Syntax

```
show snmp views [viewname]
```

- *viewname* — Specifies the name of the view. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following examples display the configuration of views with and without a view name specified.

```
console# show snmp views
```

Name	OID Tree	Type
-----	-----	-----
user-view1	1.3.6.1.2.1.1	Included
user-view1	1.3.6.1.2.1.1.7	Excluded
user-view2	1.3.6.1.2.1.2.2.1.*.1	Included

```
console# show snmp views user-view1
```

Name	OID Tree	Type
-----	-----	-----
user-view1	1.3.6.1.2.1.1	Included
user-view1	1.3.6.1.2.1.1.7	Excluded

show trapflags

Use the **show trapflags** command to show the status of the configurable SNMP traps.

Syntax

show trapflags [ospf | ospfv3]

ospf | ospfv3—Use this parameter to show detailed OSPF trap status information

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show trapflags
```

```
Authentication Flag..... Enable
Link Up/Down Flag..... Enable
Multiple Users Flag..... Enable
Spanning Tree Flag..... Enable
ACL Traps..... Disable
DVMRP Traps..... Disable
OSPFv2 Traps..... Disable
PIM Traps..... Disable
OSPFv3 Traps..... Disable
CP Traps..... Disable
```

```
console#show trapflags ospf
```

OSPF Traps:

```
errors:      all.....Disabled
             authentication failure.....Enabled
             bad packet.....Enabled
             config error.....Enabled
             virt authentication failure .....Disabled
             virt bad packet.....Disabled
             virt config error.....Disabled
if-rx:      if-rx-packet.....Disabled
lsa:        lsa-maxage.....Disabled
             lsa-originate.....Disabled
overflow:   lsdb-overflow.....Enabled
             lsdb-approaching-overflow.....Enabled
retransmit: packets.....Disabled
             virt-packets.....Disabled
rtb:        rtb-entry-info.....Disabled
state-change: all.....Disabled
             if state change.....Enabled
             neighbor state change.....Enabled
             virtif state change.....Disabled
             virtneighbor state change.....Disabled
```

snmp-server community

Use the **snmp-server community** command in Global Configuration mode to set up the community access string to permit access to the SNMP protocol. To remove the specified community string, use the **no** form of this command. This Command places the user in SNMP-Community-Configuration mode.

Syntax

snmp-server community *community-string* {**ro** | **rw** | **su**} [**ipaddress** *ipaddress*] [**view** *viewname*]

no snmp-server community *community-string*

- *community-string* — Permits access to the SNMP protocol. (Range: 1-20 characters)
- **ro** — Indicates read-only access
- **rw** — Indicates read-write access.
- **su** — Indicates SNMP administrator access.
- *ipaddress* — Specifies the IP address of the management station. If no IP address is specified, all management stations are permitted.
- *viewname* — Specifies the name of a previously defined view. For information on views, see the user guidelines. (Range: 1-30 characters)

Default Configuration

No community is defined.

Command Mode

Global Configuration mode

User Guidelines

You can not specify *viewname* for **su**, which has an access to the whole MIB. You can use the view name to restrict the access rights of a community string. When it is specified:

- An internal security name is generated.
- The internal security name for SNMPv1 and SNMPv2 security models is mapped to an internal group name.
- The internal group name for SNMPv1 and SNMPv2 security models is mapped to a view name. If **ro** is specified, then read-view and notify-view are mapped. If **rw** is specified, then read-view, notify-view, and write-view are mapped.

Example

The following example configures community access string **public** to permit administrative access to SNMP at an administrative station with IP address 192.168.1.20.

```
console(config)# snmp-server community public su  
ipaddress 192.168.1.20
```

snmp-server community-group

Use the **snmp-server community-group** command in Global Configuration mode to map the internal security name for SNMP v1 and SNMP v2 security models to the group name. To remove the specified community string, use the **no** form of this command.

Syntax

snmp-server community-group *community-string group-name* [**ipaddress** *ip-address*]

- *community-string* — Community string that acts like a password and permits access to the SNMP protocol. (Range: 1-20 characters)
- *group-name* — Name of a previously defined group. The group defines the objects available to the community. (Range: 1-30 characters)
- *ip-address* — Management station IP address. Default is all IP addresses.

Default Configuration

No community group is defined.

Command Mode

Global Configuration mode

User Guidelines

The *group-name* parameter can be used to restrict the access rights of a community string. When it is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

Example

The following example maps a community access string `dell_community` to group `dell_group`.

```
console(config)# snmp-server community-group  
dell_community dell_group 192.168.29.1
```

snmp-server contact

Use the **snmp-server contact** command in Global Configuration mode to set up a system contact (`sysContact`) string. To remove the system contact information, use the **no** form of the command.

Syntax

snmp-server contact *text*

no snmp-server contact

- *text* — Character string, 0 to 160 characters, describing the system contact information.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays setting up the system contact point as "Dell_Technical_Support".

```
console(config)# snmp-server contact  
Dell_Technical_Support
```

snmp-server enable traps

Use the **snmp-server enable traps** command to enable SNMP traps globally or to enable specific SNMP traps. Use the “no” form of this command to disable SNMP traps. See Granular OSPF v2/v3 Traps for more detail about the OSPF trap types.

Syntax

snmp-server enable traps [acl | all | authentication | captive portal | dvmrp | link | multiple users | ospf *ospftype* | ospfv3 *ospfv3type* | pim | spanning tree]

- *ospftype* - {
all |
errors {all | authentication failure | bad packet | config error | virt authentication failure | virt bad packet | virt config error} | lsa {all | lsa-maxage | lsa-originate} | overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} | state-change {all | if state change | neighbor state change | virtif state change | virtneighbor state change}
}
- *ospfv3type* - {
all |
errors {all | bad packet | config error | virt bad packet | virt config error} | lsa {all | lsa-maxage | lsa-originate} | overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} | state-change {all | if state change | neighbor state change | virtif state change | virtneighbor state change}
}

Default Configuration

Authentication, Link Up/Down, Multiple Users and Spanning Tree flags are enabled by default.

Command Mode

Global Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the options for the **snmp-server enable traps** command.

```
console(config)#snmp-server enable traps ?
```

<cr>	Press enter to execute the command.
acl	acl
all	Enable/Disable all Traps.
authentication	To enable the device to send SNMP traps when authentication fails.
dvmrp	dvmrp
link	Enable/Disable switch level Link Up/Down trap flag.
multiple-users	Enable/Disable sending traps when multiple logins active.
ospf	Enable/Disable OSPF Traps.
ospfv3	Enable/Disable OSPF Traps.
pim	pim
spanning-tree	Enable/Disable sending Spanning Tree traps.

snmp-server enable traps authentication

Use the **snmp-server enable traps authentication** command in Global Configuration mode to enable the switch to send Simple Network Management Protocol traps when authentication fails. To disable SNMP failed authentication traps, use the **no** form of this command.

Syntax

snmp-server enable traps authentication

no snmp-server enable traps authentication

Default Configuration

Traps are enabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the command to enable authentication failed SNMP traps.

```
console(config)# snmp-server enable traps
authentication
```

snmp-server engineID local

Use the **snmpserver engineID local** command in Global Configuration mode to specify the Simple Network Management Protocol (SNMP) engine ID on the local device.

To remove the configured engine ID, use the **no** form of this command.

Syntax

snmp-server engineID local {*engineid-string* | **default**}

no snmp-server engineID local

- *engineid-string* — The character string that identifies the engine ID. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 6-32 characters)
- **default** — The engineID is created automatically, based on the device MAC address.

Default Configuration

The *engineID* is not configured.

Command Mode

Global Configuration mode

User Guidelines

If you want to use SNMPv3, you need to specify an engine ID for the device. You can specify your own ID or use a default string that is generated using the MAC address of the device. If the SNMPv3 engine ID is deleted, or the configuration file is erased, then SNMPv3 cannot be used. Since the EngineID should be unique within an administrative domain, the following guidelines are recommended:

- 1 For standalone devices use the default keyword to configure the Engine ID.
- 2 For stackable systems, configure your own EngineID, and verify that is unique within your administrative domain.

Changing the value of `snmpEngineID` has important side-effects. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of `engineID` changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured.

Example

The following example configures the Engine ID automatically.

```
console(config)# snmp-server engineID local default
```

snmp-server filter

Use the **snmp-server filter** command in Global Configuration mode to create or update a Simple Network Management Protocol (SNMP) server filter entry. To remove the specified SNMP server filter entry, use the **no** form of this command.

Syntax

snmp-server filter *filter-name oid-tree* {included | excluded}

no snmp-server filter *filter-name* [*oid-tree*]

- *filter-name* — Specifies the label for the filter record that is being updated or created. The name is used to reference the record. (Range: 1-30 characters.)
- *oid-tree* — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included** — Indicates that the filter type is included.
- **excluded** — Indicates that the filter type is excluded.

Default Configuration

No filter entry exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines.

Examples

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group.

```
console(config)# snmp-server filter user-filter  
system included
```

```
console(config)# snmp-server filter user-filter  
system.7 excluded
```

```
console(config)# snmp-server filter user-filter  
ifEntry.*.1 included
```

snmp-server group

Use the **snmp-server group** command in Global Configuration mode to configure a new Simple Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. To remove a specified SNMP group, use the **no** form of this command.

Syntax

```
snmp-server group groupname {v1 | v2 | v3 {noauth | auth | priv} [notify  
notifyview]} [context contextname] [read readview] [write writeview]
```

```
no snmp-server group groupname { v1 | v2 | v3 { noauth | auth | priv } } [   
context contextname ]
```

- *groupname* — Specifies the name of the group. (Range: 1-30 characters.)
- **v1** — Indicates the SNMP Version 1 security model.
- **v2** — Indicates the SNMP Version 2 security model.
- **v3** — Indicates the SNMP Version 3 security model.
- **noauth** — Indicates no authentication of a packet. Applicable only to the SNMP Version 3 security model.
- **auth** — Indicates authentication of a packet without encrypting it. Applicable only to the SNMP Version 3 security model.
- **priv** — Indicates authentication of a packet with encryption. Applicable only to the SNMP Version 3 security model.
- *contextname* — Provides different views of the system and provides the user a way of specifying that context.
- *notifyview* — Defines a string that is the name of the view that enables specifying an inform or a trap. If unspecified, nothing is defined for the notify view. (Range: 1-30 characters.)
- *readview* — A string that is the name of the view that enables the you to view only the contents of the agent. If unspecified, all the objects except for the community-table and SNMPv3 user and access tables are available. (Range: 1-30 characters.)

- *writeview* — A string that is the name of the view that enables the user to enter data and configure the contents of the agent. If unspecified, nothing is defined for the write view. (Range: 1-30 characters.)

Default Configuration

No group entry exists. There will be some default groups for Read/Write/Super users. These groups cannot be deleted or modified by the user. This command is used only to configure the user-defined groups.

Command Mode

Global Configuration Mode

User Guidelines

View-name should be an existing view created using the **snmp-server view** command. If there are multiple records with the same view-name, then the argument specified in this command points to first view-name in the table.

Example

The following example attaches a group called **user-group** to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called **user-view**.

```
console(config)# snmp-server group user-group v3 priv  
read user-view
```

snmp-server host

Use the **snmp-server host** command in Global Configuration mode to specify the recipient of Simple Network Management Protocol notifications. To remove the specified host, use the **no** form of this command. This command enters the user into SNMP-host configuration mode.

SNMP Server Name

The existing commands **snmp-server host** <host name>, **snmp-server v3-host** <host name> do not allow spaces in a host name. It is not common practice for administrators to permit such hostnames (incompatible with various protocols), but technically, DNS could resolve the proper address.

These commands are updated to allow space(s) in host name when specified in double quotes.

Example

```
#snmp-server host "host name"  
#snmp-server v3-host "host name"
```

Syntax

snmp-server host { *ip-address* | *hostname* } *community* { **traps** { *v1* | *v2* } | **informs** [*timeout seconds*] [*retries retries*] [*udpport port*] [*filter filtername*]

no snmp-server host *ip-address* { *traps* | *informs* }

- *ip-address* — Specifies the IPv4 address of the host (targeted recipient).
- *hostname* — Specifies the name of the host. (Range: 1-158 characters)
- *community* — Specifies a password-like community string sent with the notification operation. (Range: 1-20 characters)
- **traps** — Indicates that SNMP traps are sent to this host.
- *v1* — Indicates that SNMPv1 traps will be used.
- *v2* — Indicates that SNMPv2 traps will be used.
- **informs** — Indicates that SNMPv2 informs are sent to this host.
- *seconds* — Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1-300 characters.)
- *retries* — Maximum number of times to resend an inform request. The default is 3 attempts. (Range: 0-255 characters.)
- *port* — UDP port of the host to use. The default is 162. (Range: 1-65535 characters.)
- *filtername* — A string that is the name of the filter that defines the filter for this host. If unspecified, does not filter anything (Range: 1-30 characters.)

Default Configuration

The default configuration is 3 retries, and 15 seconds timeout.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables SNMP traps for host 192.16.12.143.

```
console(config)# snmp-server host 192.16.12.143  
Dell_powerconnect traps v2
```

snmp-server location

Use the **snmp-server location** command in Global Configuration mode to set the system location string. To remove the location string, use the **no** form of this command.

Syntax

snmp-server location *text*

no snmp-server location

- *text* — Character string describing the system location. (Range: 1 to 255 characters.)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the device location as "New_York".

```
console(config)# snmp-server location New_York
```

snmp-server user

Use the **snmp-server user** command in Global Configuration mode to configure a new SNMP Version 3 user. To delete a user, use the **no** form of this command.

Syntax

snmp-server user *username* *groupname* [**remote** *engineid-string*] [{ **auth-md5** *password* | **auth-sha** *password* | **auth-md5-key** *md5-key* | **auth-sha-key** *sha-key* } [**priv-des** *password* | **priv-des-key** *des-key*]]

no snmp-server user *username*

- *username* — Specifies the name of the user on the host that connects to the agent. (Range: 1-30 characters.)
- *groupname* — Specifies the name of the group to which the user belongs. (Range: 1-30 characters.)
- *engineid-string* — Specifies the engine ID of the remote SNMP entity to which the user belongs. The engine ID is a concatenated hexadecimal string. Each byte in the hexadecimal character string is two hexadecimal digits. The remote engine id designates the remote management station, and should be defined to enable the device to receive acknowledgements to "informs." (Range: 5-32 characters.)
- **auth-md5** — The HMAC-MD5-96 authentication level.
- **auth-sha** — The HMAC-SHA-96 authentication level.
- *password* — A password. (Range: 1 to 32 characters.)
- **auth-md5-key** — The HMAC-MD5-96 authentication level. Enter a pregenerated MD5 key.
- **auth-sha-key** — The HMAC-SHA-96 authentication level. Enter a pregenerated SHA key.
- *md5-key* — Character string—length 32 hex characters.
- *sha-key* — Character string—length 48 characters.

- **priv-des** — The CBC-DES Symmetric Encryption privacy level. Enter a password.
- **priv-des-key** — The CBC-DES Symmetric Encryption privacy level. The user should enter a pregenerated MD5 or SHA key depending on the authentication level selected.
- **des-key** — The pregenerated DES encryption key. Length is determined by authentication method selected—32 hex characters if MD5 Authentication is selected, 48 hex characters if SHA Authentication is selected.

Default Configuration

No user entry exists.

Command Mode

Global Configuration mode

User Guidelines

If the SNMP local engine ID is changed, configured users will no longer be able to connect and will need to be reconfigured.

Example

The following example configures an SNMPv3 user "John" in group "user-group".

```
console(config)# snmp-server user John user-group
```

snmp-server view

Use the **snmp-server view** command in Global Configuration mode to create or update a Simple Network Management Protocol (SNMP) server view entry. To delete a specified SNMP server view entry, use the **no** form of this command.

Syntax

```
snmp-server view view-name oid-tree { included | excluded }
```

```
no snmp-server view view-name [oid-tree ]
```

- *view-name* — Specifies the label for the view record that is being created or updated. The name is used to reference the record. (Range: 1-30 characters.)
- *oid-tree* — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as *system*. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- **included** — Indicates that the view type is included.
- **excluded** — Indicates that the view type is excluded.

Default Configuration

A view entry does not exist.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view record.

Examples

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group.

```
console(config)# snmp-server view user-view system
included
```

```
console(config)# snmp-server view user-view system.7
excluded
```

```
console(config)# snmp-server view user-view
ifEntry.*.1 included
```

snmp-server v3-host

Use the **snmp-server v3-host** command in Global Configuration mode to specify the recipient of Simple Network Management Protocol Version 3 notifications. To remove the specified host, use the **no** form of this command.

Syntax

snmp-server v3-host {*ip-address* | *hostname*} *username* {**traps** | **informs**} [**noauth** | **auth** | **priv**] [**timeout** *seconds*] [**retries** *retries*] [**udpport** *port*] [**filter** *filtername*]

no snmp-server host *ip-address*

- *ip-address* — Specifies the IPv4 address of the host (targeted recipient).
- *hostname* — Specifies the name of the host. (Range: 1-158 characters.)
- *username* — Specifies user name used to generate the notification. (Range: 1-25 characters.)
- **traps** — Indicates that SNMP traps are sent to this host.
- **informs** — Indicates that SNMPv2 informs are sent to this host.
- **noauth** — Specifies sending of a packet without authentication.
- **auth** — Specifies authentication of a packet without encrypting it
- **priv** — Specifies authentication and encryption of a packet.
- *seconds* — Number of seconds to wait for an acknowledgment before resending informs. This is not allowed for hosts configured to send traps. The default is 15 seconds. (Range: 1-300 seconds.)
- *retries* — Maximum number of times to resend an inform request. This is not allowed for hosts configured to send traps. The default is 3 attempts. (Range: 0-255 retries.)
- *port* — UDP port of the host to use. The default is 162. (Range: 1-65535.)
- *filtername* — A string that is the name of the filter that define the filter for this host. If unspecified, does not filter anything. (Range: 1-30 characters.)

Default Configuration

Default configuration is 3 retries and 15 seconds timeout.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example identifies an SNMPv3 host.

```
console(config)# snmp-server v3-host 192.168.0.20
```


SSH Commands

This chapter explains the following commands:

- `crypto key generate dsa`
- `crypto key generate rsa`
- `crypto key pubkey-chain ssh`
- `ip ssh port`
- `ip ssh pubkey-auth`
- `ip ssh server`
- `key-string`
- `show crypto key mypubkey`
- `show crypto key pubkey-chain ssh`
- `show ip ssh`
- `user-key`

crypto key generate dsa

Use the **crypto key generate dsa** command in Global Configuration mode to generate DSA key pairs for your switch. A key pair is one public DSA key and one private DSA key.

Syntax

crypto key generate dsa

Default Configuration

DSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

DSA keys are generated in pairs: one public DSA key and one private DSA key. If your switch already has DSA keys when you issue this command, you are warned and prompted to replace the existing keys. The keys are not saved in the switch configuration; they are saved in the file system and the private key is never displayed to the user. DSA keys, along with other switch credentials, are distributed to all units in a stack on a configuration save.

Example

The following example generates DSA key pairs.

```
console(config)#crypto key generate dsa
```

crypto key generate rsa

Use the **crypto key generate rsa** command in Global Configuration mode to generate RSA key pairs.

Syntax

crypto key generate rsa

Default Configuration

RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

RSA keys are generated in pairs: one public RSA key and one private RSA key. If your switch already has RSA keys when you issue this command, you are warned and prompted to replace the existing keys. The keys are not saved in the switch configuration; they are saved in the file system and the private key is never displayed to the user. RSA keys, along with other switch credentials, are distributed to all units in a stack on a configuration save.

Example

The following example generates RSA key pairs.

```
console(config)#crypto key generate rsa
```

crypto key pubkey-chain ssh

Use the **crypto key pubkey-chain ssh** command in Global Configuration mode to enter public key configuration mode in order to manually specify public keys such as SSH client public keys.

Syntax

```
crypto key pubkey-chain ssh
```

Default Configuration

By default, this command has no public keys configured.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enters the SSH Public Key-chain configuration mode.

```
console#configure
```

```
console(config)#crypto key pubkey-chain ssh
```

```
console(config-pubkey-chain)#user-key bob rsa
```

```
console(config-pubkey-key)#key-String
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWlAl4kpqIw9GBRon  
ZQZxjHKcqKL6rMlQ+ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+  
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwO1lgkTwml75QR9gHujS6KwG  
N2QWXgh3ub8gDjTSqMuSn/Wd05iDX2IExQWu08licglk02LYciz+Z  
4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnkmlsh  
RE7Di71+w3fNiOA6w9o44t6+AINEICBCCA4YcF6zMzaTlwefWwX6f  
+Rmt5nhhqdAtN/4oJfce166DqVX1gWmNzNR4DYDvSzg0lDnwCAC8Q  
h
```

```
console(config-pubkey-key)#exit
```

ip ssh port

Use the **ip ssh port** command in Global Configuration mode to specify the TCP port to be used by the SSH server. To use the default port, use the **no** form of this command.

Syntax

```
ip ssh port port-number
```

```
no ip ssh port
```

- *port-number* — Port number for use by the SSH server. (Range: 1–65535)

Default Configuration

The default value is 22.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the port to be used by the SSH server as 8080.

```
console(config)#ip ssh port 8080
```

ip ssh pubkey-auth

Use the **ip ssh pubkey-auth** command in Global Configuration mode to enable public key authentication for incoming SSH sessions. To disable this function, use the **no** form of this command.

Syntax

ip ssh pubkey-auth

no ip ssh pubkey-auth

Default Configuration

The function is disabled.

Command Mode

Global Configuration mode

User Guidelines

AAA authentication is independent from this configuration.

Example

The following example enables public key authentication for incoming SSH sessions.

```
console(config)#ip ssh pubkey-auth
```

ip ssh server

Use the **ip ssh server** command in Global Configuration mode to enable the switch to be configured from SSH. To disable this function, use the **no** form of this command.

Syntax

ip ssh server

no ip ssh server

Default Configuration

This command is **enabled** by default.

Command Mode

Global Configuration mode

User Guidelines

To generate SSH server keys, use the commands **crypto key generate rsa**, and **crypto key generate dsa**.

Example

The following example enables the switch to be configured using SSH.

```
console(config)#ip ssh server
```

key-string

Use the **key-string** SSH Public Key Configuration mode to specify an SSH public key manually.

Syntax

key-string *key-string*

key-string row *key-string*

- **row** — To specify the SSH public key row by row.
- *key-string* — The UU-encoded DER format is the same format as the authorized keys file used by OpenSSH.

Default Configuration

By default, the key-string is empty.

Command Mode

SSH Public Key Configuration mode

User Guidelines

Use the **key-string row** command to specify which SSH public key you will configure interactively next. To complete the interactive command, you must enter **key-string row** with no characters.

Examples

The following example shows how to enter a public key string for a user called "bob."

```
console(config)#crypto key pubkey-chain ssh
console(config-pubkey-chain)#user-key bob rsa
console(config-pubkey-key)#key-string
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWl
Al4kppqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOllg
kTwm175QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licg1k02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di7l+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaTlwefWwX6f+
Rmt5nhhqdaTn/4oJfce166DqVXlgWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint:
a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

```
console(config)#crypto key pubkey-chain ssh
console(config-pubkey-chain)#user-key bob rsa
console(config-pubkey-key)#key-string row AAAAB3Nza
console(config-pubkey-key)#key-string row C1yc2
```

show crypto key mypubkey

Use the `show crypto key mypubkey` command in Privileged EXEC mode to display the SSH public keys of the switch.

Syntax

```
show crypto key mypubkey [rsa|dsa]
```

- `rsa` — RSA key.
- `dsa` — DSA key.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the SSH public keys on the switch.

```
console#show crypto key mypubkey rsa
rsa key data:
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAu7WhtjQDUygjSQXHVgyqdUby
```



```
dxUXEAiDHXcWHVr0R/ak1HDQitBzeEv1vVEToen5ddLmRhtIgrdKU
JHgBHJV
```

```
R2VaSN/WC0IK53j9re4B11AE+O3qAxwJs0KD7cTkVF9I+YdiXeOM8
VE4skkw
```

```
AiyLDNVWXgNQ6iat8+8Mjth+PIo5t3HykYUCkD8B1v93nzi/sr4hH
HJCdx7w
```

```
wRW3QtgXaGwYt2rdlr3x8ViAF6B7AKYd8xGVVjyJTD6TjrCRRwQHg
B/BHsFr
```

```
z/R1lSYa0vFje1/7/0qaIDSHfHqWhajYkMa4xPOtIye7oqzAOm1b7
6l28uTB
```

```
luBEoLQ+PKOKMiK8sQ==
```

Fingerprint (hex) :

```
58:7f:5c:af:ba:d3:60:88:42:00:b0:2f:f1:5a:a8:fc
```

Fingerprint (bubbleBabble) : xodob-liboh-heret-tiver-
dyrib-godac-pynah-muzyt-mofim-bihog-cuxyx

show crypto key pubkey-chain ssh

Use the `show crypto key pubkey-chain ssh` command in Privileged EXEC mode to display SSH public keys stored on the switch.

Syntax

`show crypto key pubkey-chain ssh [username username] [fingerprint bubble-babble|hex]`

- *username* — Specifies the remote SSH client username. (Range: 1–48 characters)
- *bubble-babble* — Fingerprints in Bubble Babble format.
- *hex* — Fingerprint in Hex format. If fingerprint is unspecified, it defaults to Hex format.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays all SSH public keys stored on the switch.

```
console#show crypto key pubkey-chain ssh
```

```
Username    Fingerprint
```

```
-----
```

```
bob          9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F
1:86
```

```
john         98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:8
7:C8
```

The following example displays the SSH public called "dana."

```
console#show crypto key pubkey-chain ssh username dana
```

```
Username: dana
```

```
rsa key data:
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAABIwAAAIEAywqRKTRnexcckxVUVTeMl+Gkh
```

```
imyUDhcTkgeFssLPMsgoXlTwzCE5+97UIIsSRKQQWR+pBNl45tCYd
75LUofV
```

```
4LP6LjlQ5Q0w5lBgiqC2MZ/iBHGSsHMAE0lpYtelZprDu4uiZHMuW
ezmdQp9
```

```
a1PU4jwQ22Tlcfauq3sqC3FMUoU=
```

```
Fingerprint:
```

```
2f:09:e7:6f:c9:bf:ab:04:d4:6f:a0:eb:e8:df:7a:11
```

show ip ssh

Use the `show ip ssh` command in Privileged EXEC mode to display the SSH server configuration.

Syntax

`show ip ssh`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the SSH server configuration.

```
console#show ip ssh
```

```
SSH server enabled. Port: 22
```

```
RSA key was generated.
```

```
DSA key was generated.
```

```
SSH Public Key Authentication is enabled.
```

```
Active incoming sessions:
```

IP Address Time	User Name SessionTime	Idle
-----	-----	-----
10.240.1.122	John	
	00:00:00	00:00:08

user-key

Use the **user-key** command in SSH Public Key Chain Configuration mode to specify which SSH public key you are configuring manually. To remove a SSH public key, use the **no** form of this command.

Syntax

user-key *username* {**rsa** | **dsa**}

no user-key *username*

- *username* — Specifies the remote SSH client username. (Range: 1–48 characters)
- **rsa** — RSA key
- **dsa** — DSA key

Default Configuration

By default, there are no keys.

Command Mode

SSH Public Key Chain Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables a SSH public key to be manually configured for the SSH public key chain called "bob."

```
console(config)#crypto key pubkey-chain ssh
console(config-pubkey-chain)#user-key bob rsa
console(config-pubkey-key)#
```

Syslog Commands

This chapter explains the following commands:

- clear logging
- clear logging file
- description
- level
- logging
- logging buffered
- logging console
- logging facility
- logging file
- logging on
- logging snmp
- logging web-session
- port
- show logging
- show logging file

clear logging

Use the **clear logging** command in Privileged EXEC mode to clear messages from the internal logging buffer.

Syntax

clear logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example clears messages from the internal syslog message logging buffer.

```
console#clear logging
```

```
Clear logging buffer [y/n]
```

clear logging file

Use the **clear logging file** command in Privileged EXEC mode to clear messages from the logging file.

Syntax

clear logging file

Default Configuration

There is no default configuration for the command.

Command Mode

Privileged EXEC

User Guidelines

This command has no user guidelines.

Example

The following example shows the **clear logging file** command and confirmation response.

```
console#clear logging file
Clear logging file [y/n]
```

description

Use the **description** command in Logging mode to describe the syslog server.

Syntax

description *description*

- *description* — Sets the description of the syslog server. (Range: 1-64 characters.)

Default Configuration

This command has no default value.

Command Mode

Logging mode

User Guidelines

After entering the view corresponding to a specific syslog server, the command can be executed to set the description of the server.

Example

The following example sets the syslog server description.

```
console(config-logging)#description "syslog server 1"
```

level

Use the **level** command in Logging mode to specify the importance level of syslog messages. To reset to the default value, use the **no** form of the command.

Syntax

level *level*

no level

- *level* — The level number for syslog messages. (Range: **emergency**, **alert**, **critical**, **error**, **warning**, **notice**, **info**, **debug**)

Default Configuration

The default value for *level* is **info**.

Command Mode

Logging mode

User Guidelines

After entering the view corresponding to a specific syslog server, the command can be executed to set the importance level for syslog messages.

Example

The following example sets the syslog message importance level to alert.

```
console(config-logging)#level alert
```

logging cli-command

Use the **logging cli-command** in Global Configuration mode to enable CLI command logging.

Syntax

logging cli-command

no logging cli-command

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

To see the CLI commands by using the **show logging** command.

Example

```
console(config)#logging cli-command
<189> JAN 13 05:20:27 192.168.2.1-1 UNKN[248900192]:
cmd_logger_api.c(87) 2113 %% CLI:EIA-
232:----:vlan 3
<189> JAN 13 05:20:27 192.168.2.1-1 UNKN[248900192]:
cmd_logger_api.c(87) 2114 %% CLI:EIA-
232:----:ex
<189> JAN 13 05:20:28 192.168.2.1-1 UNKN[248900192]:
cmd_logger_api.c(87) 2115 %% CLI:EIA-
232:----:
<189> JAN 13 05:20:39 192.168.2.1-1 UNKN[248900192]:
cmd_logger_api.c(87) 2116 %% CLI:EIA-
232:----:show logging file
```

logging

Use the **logging** command in Global Configuration mode to log messages to a syslog server. To delete the syslog server with the specified address from the list of syslogs, use the **no** form of this command.

Syntax

```
logging {ip-address | hostname}
```

no logging {*ip-address* | *hostname*}

- *ip-address* — IP address of the host to be used as a syslog server.
- *hostname* — Hostname of the host to be used as a syslog server. (Range: 1-158 characters)

Default Configuration

No syslog servers defined.

Command Mode

Global Configuration mode

User Guidelines

Up to eight syslog servers can be used.

Example

The following example places the designated server in logging configuration mode.

```
console(config)#logging 192.168.15.1
```

logging buffered

Use the **logging buffered** command in Global Configuration mode to limit syslog messages displayed from an internal buffer based on severity. To cancel the buffer use, use the **no** form of this command.

Syntax

logging buffered *level*

no logging buffered

- *level* — Limits the message logging to a specified level buffer. (Range: emergency, alert, critical, error, warning, notice, info, debug)

Default Configuration

The default value for *level* is **info**.

Command Mode

Global Configuration mode

User Guidelines

All the syslog messages are logged to the internal buffer. This command limits the commands displayed to the user.

Example

The following example limits syslog messages displayed from an internal buffer based on the severity level "error."

```
console(config)#logging buffered error
```

logging console

Use the **logging console** command in Global Configuration mode to limit messages logged to the console based on severity. To disable logging to the console terminal, use the **no** form of this command.

Syntax

logging console *level*

no logging console

- *level*— Limits the logging of messages displayed on the console to a specified level. (Range: **emergency**, **alert**, **critical**, **error**, **warning**, **notice**, **info**, **debug**)

Default Configuration

The default value for *level* is **info**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example limits messages logged to the console based on severity level "alert".

```
console(config)#logging console alert
```

logging facility

Use the **logging facility** command in Global Configuration mode to set the facility for logging messages. To reset to the default value, use the **no** form of the command.

Syntax

logging facility *facility*

no logging facility

- *facility* — The facility that will be indicated in the message. (Range: local0, local1, local2, local3, local4, local5, local 6, local7)

Default Configuration

The default value is **local7**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the logging facility as **local3**.

```
console(config)#logging facility local3
```

logging file

Use the **logging file** command in Global Configuration mode to limit syslog messages sent to the logging file based on severity. To cancel the buffer, use the **no** form of this command.

Syntax

logging file *level*

no logging file

- *level*— Limits the logging of messages to the buffer to a specified level. (Range: emergency, alert, critical, error, warning, notice, info, debug)

Default Configuration

The default value for *level* is **error**.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example limits syslog messages sent to the logging file based on the severity level "warning."

```
console(config)#logging file warning
```

logging on

Use the **logging on** command in Global Configuration mode to control error messages logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. To disable the logging process, use the **no** form of this command.

Syntax

logging on

no logging on

Default Configuration

Logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server. Logging on and off for these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging <server>** global configuration commands. However, if the **logging on** command is disabled, no messages are sent to these destinations. Only the console receives messages.

Example

The following example shows how logging is enabled.

```
console(config)#logging on
```

logging snmp

Use the **logging snmp** command in Global Configuration mode to enable SNMP Set command logging. To disable, use the no form of this command.

Syntax

logging snmp

no logging snmp

Default Configuration

Disabled.

Command Mode

Global Configuration mode

User Guidelines

To see SNMP Set command logs use the show logging command.

Example

```
console(config)#logging snmp
```

logging web-session

Use the **logging web-session** command in Global Configuration mode to enable web session logging. To disable, use the no form of this command.

Syntax

logging web-session

no logging web-session

Default Configuration

Disabled.

Command Mode

Global Configuration mode

User Guidelines

To see web session logs use the show logging command.

Example

```
console(config)#logging web-session
```

```
<133> MAR 24 07:46:07 10.131.7.165-2 UNKN[83102768]:  
cmd_logger_api.c(140) 764 %%  
WEB:10.131.7.67:<<UNKNOWN>>:EwaSessionLookup :  
session[0] created
```

```
<133> MAR 24 07:46:07 10.131.7.165-2 UNKN[83102768]:  
cmd_logger_api.c(140) 765 %%  
WEB:10.131.7.67:admin:User admin logged in
```

port

Use the **port** command in Logging mode to specify the port number of syslog messages. To reset to the default value, use the **no** form of the command.

Syntax

port *port*

no port

- port — The port number for syslog messages. (Range: 1-65535)

Default Configuration

The default port number is 514.

Command Mode

Logging mode

User Guidelines

After entering the view corresponding to a specific syslog server, the command can be executed to set the port number for the server.

Example

The following example sets the syslog message port to 300.

```
console(config-logging)#port 300
```

show logging

Use the **show logging** command in Privileged EXEC mode to display the state of logging and the syslog messages stored in the internal buffer.

Syntax

show logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the state of logging and the syslog messages stored in the internal buffer.

```
console#show logging
```

```
Logging is enabled.
```

```
Console logging: level debugging. console Messages: 0  
Dropped.
```

```
Buffer logging: level debugging. Buffer Messages: 11 Logged,  
200 Max.
```

```
File logging: level notifications. File Messages: 0 Dropped.
```

```
Syslog server 192.180.2.27 logging: errors. Messages: 6  
Dropped.
```

```
console#show logging
```

```
Console logging: level warning. Console Messages: 2100  
Dropped.
```

```
Buffer Logging: level info. Buffer Messages: 2100 Logged,  
200 Max
```

```
File Logging: level notActive. File Messages: 0 Dropped.
```

```
CLI Command Logging : disabled
```

```
Web Session Logging : disabled
```

```
SNMP Set Command Logging : disabled
```

```
366 Messages were not logged.
```

```
Buffer Log:
```

```
<189> JAN 10 10:44:49 192.168.2.1-1 TRAPMGR[232224784]:  
traputil.c(910) 1901 %% Spanning Tree Topology Change: 14,  
Unit: 1
```

```
Syslog server 192.180.2.28 logging: errors. Messages: 6  
Dropped.
```

```
2 messages were not logged (resources)
```

```
Buffer log:
```

```
11-Aug-2005 15:41:43: %LINK-3-UPDOWN: Interface  
FastEthernet g1, changed state to up
```

```
11-Aug-2005 15:41:43: %LINK-3-UPDOWN: Interface Ethernet
g1, changed state to up
11-Aug-2005 15:41:43: %LINK-3-UPDOWN: Interface Ethernet
g1, changed state to up
11-Aug-2005 15:41:43: %LINK-3-UPDOWN: Interface Ethernet
g2, changed state to up
11-Aug-2005 15:41:43: %LINK-3-UPDOWN: Interface Ethernet
g3, changed state to up
11-Aug-2005 15:41:43: %SYS-5-CONFIG_I: Configured from
memory by console
11-Aug-2005 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet g1, changed state to up
11-Aug-2005 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g1, changed state to down
11-Aug-2005 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g1, changed state to down
11-Aug-2005 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet g2, changed state to down
11-Aug-2005 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet 1/3, changed state to down
```

show logging file

Use the **show logging file** command in Privileged EXEC mode to display the state of logging and the syslog messages stored in the logging file.

Syntax

show logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the state of logging and syslog messages sorted in the logging file.

```
console#show logging file
Persistent Logging : enabled
Persistent Log Count : 1
<186> JAN 01 00:00:05 0.0.0.0-1 UNKN[268434928]:
bootos.c(382) 3 %% Event(0xaaaaaaaa)
```

show syslog-servers

Use the **show syslog-servers** command in Privileged EXEC mode to display the syslog servers settings.

Syntax

show syslog-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the syslog server settings.

```
console#show syslog-servers
```

IP address	Port	Severity	Facility	Description

192.180.2.275	14	Info	local7	7
192.180.2.285	14	Warning	local7	7

System Management Commands

This chapter explains the following commands:

- `asset-tag`
- `banner motd`
- `banner motd acknowledge`
- `clear checkpoint statistics`
- `cut-through mode`
- `hostname`
- `initiate failover`
- `member`
- `movemanagement`
- `no standby`
- `nsf`
- `ping`
- `reload`
- `set description`
- `show boot-version`
- `show checkpoint statistics`
- `show cut-through mode`
- `show memory cpu`
- `show nsf`
- `show process cpu`
- `show sessions`
- `show stack-port`
- `show stack-port counters`
- `show stack-port diag`
- `show stack-standby`

- show supported switchtype
- show switch
- show system
- show system id
- show tech-support
- show users
- show version
- stack
- stack-port
- standby
- switch priority
- switch renumber
- telnet
- traceroute

asset-tag

Use the **asset-tag** command in Global Configuration mode to specify the switch asset tag. To remove the existing asset tag, use the **no** form of the command.

Syntax

asset-tag [*unit*] *tag*

no asset-tag [*unit*]

- *unit*— Switch number. (Range: 1–12)
- *tag*— The switch asset tag.

Default Configuration

No asset tag is defined by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the switch asset tag as lqwepot. Because the unit parameter is not specified, the command defaults to the master switch number.

```
console(config)# asset-tag lqwepot
```

banner motd

Use the **banner motd** command to control (enable or disable) the display of message-of-the-day banners. **banner motd** enables the banner, and allows configuration of message-of-the-day banners. Use **no banner motd** to delete the message, and disable the banner.

Syntax

banner motd

no banner motd

Default Configuration

The banner is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console(config)# banner motd "IMPORTANT: There is a  
power shutdown at 23:00hrs today, duration 1 hr 30  
minutes."
```

When the MOTD banner is executed, the following displays:

```
IMPORTANT: There is a power shutdown at 23:00hrs today, duration 1 hr 30  
minutes.
```

banner motd acknowledge

The banner displayed on the console must be acknowledged if **banner motd acknowledge** is executed. Enter "y" or "n" to continue to the login prompt. If "n" is entered, the session is terminated and no further communication is allowed on that session. However, serial connection will not get terminated if 'y' is not entered. Use the **no banner motd acknowledge** command to disable banner acknowledge.

Syntax

banner motd acknowledge

no banner motd acknowlege

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

```
console(config)# banner motd "There is a power shutdown at 23:00hrs today,  
duration 1 hr 30 minutes."
```

```
console(config)# banner motd acknowledge
```

When the MOTD banner is executed, the following displays:

IMPORTANT: There is a power shutdown at 23:00hrs today, duration 1 hr 30 minutes.

Press 'y' to continue

If 'y' is entered, the following displays:

```
console >
```

If 'n' is entered, the session will get disconnected, unless it is a serial connection.

clear checkpoint statistics

Use the **clear checkpoint statistics** command to clear the statistics for the checkpointing process.

Syntax

```
clear checkpoint statistics
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

When nonstop forwarding is enabled on a stack, the stack's management unit checkpoints operational data to the backup unit. If the backup unit takes over as the management unit, the control plane on the new management unit uses the checkpointed data when initializing its state. Checkpoint statistics track the amount of data checkpointed from the management unit to the backup unit.

Example

```
console#clear checkpoint statistics
```

cut-through mode

Use the **cut-through mode** command to enable the cut-through mode on the switch. The mode takes effect on all ports on next reload of the switch. To disable the cut-through mode on the switch, use the no form of this command.

Syntax

cut-through mode

no cut-through mode

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

User Guidelines

No specific guidelines.

Example

```
console(config)#cut-through mode
```

The mode (enable) is effective from the next reload of Switch/Stack.

hostname

Use the **hostname** command in Global Configuration mode to specify or modify the switch host name. To restore the default host name, use the **no** form of the command.

Syntax

hostname *name*

no hostname

- *name* — The name of the host. (Range: 1–255 characters)

Default Configuration

Host name not configured.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example specifies the switch host name.

```
console(config)# hostname Dell
```

initiate failover

To manually force a failover from the management unit to the backup unit in a stack, use the **initiate failover** command in Stack Configuration mode.

Syntax

This command has no user guidelines.

Default Configuration

There is no default configuration.

Command Mode

Stack Configuration mode

User Guidelines

This command forces a warm restart of the stack. The backup unit takes over as the new management unit without clearing the hardware state on any of the stack members. The original management unit reboots. If the system is not ready for a warm restart, for example because no backup unit has been elected or one or more members of the stack do not support nonstop forwarding, the command fails with a warning message.

The **movemanagement** command also transfers control from the current management unit; however, the hardware is cleared and all units reinitialize.

Example

```
console(config-stack)#initiate failover ?
```

```
<cr> Press enter to execute the command.
```

```
console(config-stack)#initiate failover
```

```
Management unit will be reloaded.
```

```
Are you sure you want to failover to the backup unit?  
(y/n) y
```

member

Use the **member** command in Stack Global Configuration mode to configure the switch. Execute this command on the Management Switch. To remove a switch from the stack, use the **no** form of the command.



NOTE: The "no" form of the command may not be used if the member is present in the stack.

Syntax

member *unit switchindex*

no member *unit*

- *unit*— The switch identifier of the switch to be added or removed from the stack. (Range: 1–12)
- *switchindex*— The index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer.

Default configuration

This command has no defaults.

Command Mode

Stack Global Configuration

User Guidelines

The switch index can be obtained by executing the **show supported switchtype** command in User Exec mode.

Example

The following example displays how to add to stack switch number 2 with index 1.

```
console(config)# stack
console(config-stack)# member 2 1
```

movemanagement

Use the **movemanagement** command in Stack Global Configuration mode to move the Management Switch functionality from one switch to another.

Syntax

movemanagement *fromunit tounit*

- *fromunit*— The switch identifier on the current Management Switch.
- *tounit*— The switch identifier on the new Management Switch.

Default Configuration

This command has no default configuration.

Command Mode

Stack Global Configuration mode

User Guidelines

Upon execution, the entire stack, including all interfaces in the stack, are unconfigured and reconfigured with the configuration on the new Management Switch.

After the reload is complete, all stack management capability must be performed on the new Management Switch.

To preserve the current configuration across a stack move, execute the `copy` configuration command before performing the stack move. A stack move causes all routes and layer 2 addresses to be lost. This command is executed on the Management Switch. The administrator is prompted to confirm the management move.

Example

The following example displays how to move the Management Switch functionality from switch “1” to switch “8.”

```
console(config)#stack
console(config)#movemanagement 1 2
```

no standby

Use the `no standby` command to unconfigure the standby in the stack. In this case, FASTPATH automatically selects a standby from the existing stack units.

Syntax

`no standby`

Default Configuration

This command has no default configuration.

Command Mode

Stack Global Configuration

User Guidelines

No specific guidelines.

Example

```
console(config)#stack
```

```
console(config-stack)#no standby
```

Fastpath will automatically select a standby

nsf

Use this command to enable non-stop forwarding. The “no” form of the command will disable NSF.

Syntax

`nsf`

`no nsf`

Default Configuration

Non-stop forwarding is enabled by default.

Command Mode

Stack Global Configuration mode

User Guidelines

Nonstop forwarding allows the forwarding plane of stack units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the stack management unit.

Example

```
console(config)#nsf
```

ping

Use the `ping` command in User EXEC mode to check the accessibility of the desired node on the network.

Syntax

`ping [ip | ipv6] ipaddress | hostname [repeat count] [timeout interval] [size size]`

- *ipaddress* — IP address to ping (contact).
- *hostname* — Hostname to ping (contact) (Range: 1–158 characters).
- *count* — Number of packets to send (Range: 1–15 packets).

- *interval*— The time between Echo Requests, in seconds (Range: 1–60 seconds).
- *size* — Number of data bytes in a packet (Range: 0–65507 bytes).

Default Configuration

The default count is 4.

The default interval is 3 seconds.

The default size is 0 data bytes.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Examples

The following example displays a ping to IP address 10.1.1.1.

```
console>ping 10.1.1.1
```

```
Pinging 10.1.1.1 with 64 bytes of data:
```

```
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
```

```
----10.1.1.1 PING Statistics----
```

```
4 packets transmitted, 4 packets received, 0% packet  
loss
```

```
round-trip (ms) min/avg/max = 7/8/11
```

```
console>
```

The following example displays a ping to yahoo.com.

```
console#ping yahoo.com
Pinging yahoo.com [66,217,71,198] with 64 bytes of
data;
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet
loss
round-trip (ms) min/avg/max = 7/8/11
```

reload

Use the **reload** command in Privileged EXEC mode to reload stack members.

Syntax

reload [*unit*]

- *unit* — Unit number to be reloaded.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

If no unit is specified, all units are reloaded.

Example

The following example displays how to reload the stack.

```
console#reload 1
```

Management switch has unsaved changes.

Would you like to save them now? (y/n) **n**

Configuration Not Saved!

Are you sure you want to reload the switch? (y/n) **y**

Reloading management switch 1.

set description

Use the **set description** command in Stack Global Configuration mode to associate a text description with a switch in the stack.

Syntax

set description *unit description*

- *unit* — The switch identifier. (Range: 1–12)
- *description* — The text description. (Range: 1–80 alphanumeric characters)

Default Configuration

This command has no default configuration.

Command Mode

Stack Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example displays

```
console(config)#stack
```

```
console(config-stack)#set description 1 "unit 1"
```

show boot-version

Use the **show boot-version** command to display the boot image version details. The details available to the user include the build date and time.

Syntax

show boot-version [*unit*]

- *unit* — The switch identifier. (Range: 1–12)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC or Privileged EXEC

User Guidelines

No specific guidelines.

Example

```
console#show boot-version
unit          Boot Image Version
1             Thu Aug 30 12:01:04 2007
```

show checkpoint statistics

Use the **show checkpoint statistics** command to display the statistics for the checkpointing process.

Syntax

show checkpoint statistics

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

When nonstop forwarding is enabled on a stack, the stack's management unit checkpoints operational data to the backup unit. If the backup unit takes over as the management unit, the control plane on the new management unit uses the checkpointed data when initializing its state. Checkpoint statistics track the amount of data checkpointed from the management unit to the backup unit.

Example

```
console#show checkpoint statistics
```

```
Messages Checkpointed.....6708
Bytes Checkpointed.....894305
Time Since Counters Cleared.....3d 01:05:09
Checkpoint Message Rate.....0.025
msg/sec
Last 10-second Message Rate.....0 msg/sec
Highest 10-second Message Rate.....8 msg/sec
```

show cut-through mode

Use the `show cut-through mode` command to show the cut-through mode on the switch.

Syntax

```
show cut-through mode
```

Command Mode

Privileged EXEC

Default Configuration

This command has no default configuration.

User Guidelines

No specific guidelines.

Example

```
Console#show cut-through mode
```

```
Current mode      : Enable
```

```
Configured mode  : Disable (This mode is effective on  
next reload)
```

show memory cpu

Use the `show memory cpu` command to check the total and available RAM space on the switch.

Syntax

```
show memory cpu
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

User Guidelines

No specific guidelines.

Example

```
console#show memory cpu
```

```
Total Memory.....
262144 KBytes

Available Memory Space.....
121181 KBytes
```

show nsf

Use the `show nsf` command to show the status of non-stop forwarding.

Syntax

`show nsf`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

```
console#show nsf
```

```
Administrative Status..... Enable
Operational Status..... Enable
Last Startup Reason..... Warm Auto-
Restart
Time Since Last Restart..... 0 days 16
hrs 52 mins 55 secs
Restart In Progress..... No
Warm Restart Ready..... Yes
```

Copy of Running Configuration to Backup Unit:

```
Status..... Stale
Time Since Last Copy..... 0 days 4 hrs
53 mins 22 secs
Time Until Next Copy..... 28 seconds
```

Unit	NSF Support
----	-----
1	Yes
2	Yes
3	Yes

show process cpu

Use the `show process cpu` command to check the CPU utilization for each process currently running on the switch.

Syntax

`show process cpu`

Command Mode

Privileged EXEC

Default Configuration

This command has no default configuration.

User Guidelines

No specific guidelines.

Example

```
console#show process cpu
```

Memory Utilization Report


```

status      bytes
-----
    free    64022608
    alloc   151568112

```

CPU Utilization:

PID	Name	5 Sec	1 Min	5 Min
328bb20	tTffsPTask	0.00%	0.00%	0.02%
3291820	tNetTask	0.00%	0.00%	0.01%
3295410	tXbdService	0.00%	0.00%	0.03%
347dcd0	ipnetd	0.00%	0.00%	0.01%
348a440	osapiTimer	1.20%	1.43%	1.21%
358ee70	bcmL2X.0	0.40%	0.30%	0.12%
359d2e0	bcmCNTR.0	0.80%	0.42%	0.50%
3b5b750	bcmRX	0.00%	0.13%	0.12%
3d3f6d0	MAC Send Task	0.00%	0.07%	0.10%
--More-- or (q)uit				
3d48bd0	MAC Age Task	0.00%	0.00%	0.03%
40fdbf0	bcmLINK.0	0.00%	0.14%	0.46%
4884e70	tL7Timer0	0.00%	0.06%	0.02%
48a1250	osapiMonTask	0.00%	0.32%	0.17%
4969790	BootP	0.00%	0.00%	0.01%
4d71610	dtlTask	0.00%	0.06%	0.05%
4ed00e0	hapiRxTask	0.00%	0.06%	0.03%
562e810	DHCP snoop	0.00%	0.00%	0.06%
58e9bc0	Dynamic ARP Inspection	0.00%	0.06%	0.03%

62038a0	dot1s_timer_task	0.00%	0.00%	0.03%
687f360	dot1xTimerTask	0.00%	0.06%	0.07%
6e23370	radius_task	0.00%	0.00%	0.01%
6e2c870	radius_rx_task	0.00%	0.06%	0.03%
7bc9030	spmTask	0.00%	0.09%	0.01%
7c58730	ipMapForwardingTask	0.00%	0.06%	0.03%
7f6eee0	tRtrDiscProcessingTask	0.00%	0.00%	0.01%
b1516d0	dnsRxTask	0.00%	0.00%	0.01%
b194d60	tCptvPrtl	0.00%	0.06%	0.03%
b585770	isdPTask	0.00%	0.00%	0.02%
bda6210	RMONTask	0.00%	0.11%	0.11%
bdb24b0	boxs Req	0.00%	0.13%	0.10%
c2d6db0	sshd	0.00%	0.00%	0.01%

--More-- or (q)uit				
Total CPU Utilization		2.40%	3.62%	3.45%

show sessions

Use the `show sessions` command in Privileged EXEC mode to display a list of the open telnet sessions to remote hosts.

Syntax

`show sessions`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a list of open telnet sessions to remote hosts.

```
console#show sessions
```

Connection	Host	Address	Port
-----	-----	-----	-----
1	Remote switch	172.16.1.1	23
2	172.16.1.2	172.16.1.2	23

The following table describes the significant fields shown in the display.

Field	Description
Connection	Connection number
Host	Remote host to which the switch is connected through a Telnet session
Address	IP address of the remote host
Port	Telnet TCP port number

show stack-port

Use the `show stack-port` command in Privileged EXEC mode to display summary stack-port information for all interfaces.

Syntax

`show stack-port`

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the summary stack-port.

```
console#show stack-port
..... .Configured Running
      Stack      Stack      Link      Link
Unit  Interface Mode      Mode      Status    Speed
(Gb/s)
-----
1      xg1      Stack      Stack      Link Down    12
1      xg2      Stack      Stack      Link Down    12
1      xg3      Ethernet  Ethernet  Link Down    10
1      xg4      Ethernet  Ethernet  Link Down    10
```

The following table explains the fields in the example.

Field	Description
Interface	Unit/Port
Configured Stack Mode	Stack or Ethernet
Running Stack Mode	Stack or Ethernet
Link Status	Status of the link
Link Speed	Speed (Gb/sec) of the stack port link

show stack-port counters

Use the **show stack-port counters** command in Privileged EXEC mode to display summary data counter information for all interfaces.

Syntax

show stack-port counters

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the summary stack-port counters.

```
console#show stack-port counters
-----TX-----RX-----
      Data   Error      Data   Error
Unit  Interface Rate   Rate   Total Rate   Rate   Total
-----
1      xg1      0      0      0      0      0      0
1      xg2      0      0      0      0      0      0
1      xg3      0      0      0      0      0      0
1      xg4      0      0      0      0      0      0
```

The following table describes the fields in the example.

Field	Description
Unit	Unit
Interface	Port
Tx Data Rate	Transmit data rate in megabits per second on the stacking port.
Tx Error Rate	Platform-specific number of transmit errors per second.
Rx Data Rate	Receive data rate in megabits per second on the stacking port.
Rx Error Rate	Platform-specific number of receive errors per second.
Rx Total Errors	Platform-specific number of total receive errors since power-up.

show stack-port diag



NOTE: This command is intended only for Field Application Engineers (FAE) and developers. An FAE will advise when to run this command and capture this information.

Use the **show stack-port diag** command in Privileged EXEC mode to display front panel stacking diagnostics for each port.

Syntax

show stack-port diag

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays information about the front panel stacking diagnostics.

```
console#show stack-port diag
```

```
1/xg1:
```

```
RBYT:0 RPKT:0 TBYT:e38b50 TPKT:d1ba
```

```
RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0
```

```
console#show stack-port diag
```

```
1/xg2:
```

```
RBYT:0 RPKT:0 TBYT:e38b50 TPKT:d1ba
```

```
RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0
```

Legend:

RBYT : Received Bytes
RPKT : Received Packets
TBYT : Transmitted Bytes
TPKT : Transmitted Packets
RFCS : Received Frame Check Sequence Errors
RFRG : Received Fragment Errors
RJBR : Received Jabber Errors
RUND : Received Underrun Errors
ROVR : Received Overrun Errors
TFCS : Transmit Frame Check Sequence Errors
TERR : Transmit Errors

1 - xg1:

RBYT:148174422 RPKT:528389 TBYT:679827058
TPKT:2977561
RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0
TFCS:0 TERR:0

1 - xg2:

RBYT:0 RPKT:0 TBYT:419413311 TPKT:620443
RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0
TFCS:0 TERR:0

The following table describes the fields in the example.

Field	Description
Interface	Port
Diagnostic Entry 1	80 character string used for diagnostics
Diagnostic Entry 2	80 character string used for diagnostics
Diagnostic Entry 3	80 character string used for diagnostics

show stack-standby

Use the **show stack-standby** command to show the Standby configured in the stack. The **show stack-standby** command shows the configured or automatically selected standby unit number.

Syntax

show stack-standby

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC or User EXEC

User Guidelines

No specific guidelines.

Example

```
console>show stack-standby
standby unit: 3
```

show supported switchtype

Use the `show supported switchtype` command in User EXEC mode to display information about all supported switch types.

Syntax

`show supported switchtype` [*switchindex*]

- switchindex* — Specifies the index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer. (Range: 0–65535)

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays the information for supported switch types.

```
console>show supported switchtype
```

		Mgmt	Cod
e			
SID	Switch Model		
ID	Pref	Type	

1		0x100b000	
2	PCT6248	1	
0x100b000			

The following table describes the fields in the example.

Field	Description
Switch Index (SID)	This field displays the index into the database of supported switch types. This index is used when preconfiguring a member to be added to the stack.
Model Identifier	This field displays the model identifier for the supported switch type.
Management Preference	This field indicates the management preference value of the switch type.
Code Version	This field displays the code load target identifier of the switch type.

The following example displays the format of the **show supported switchtype** [*switchindex*] command.

```
console#show supported switchtype 1
Switch Type..... 0x73950001
Model Identifier..... 6224
Switch Description..... PowerConnect 6224
Management Preference..... 1
Expected Code Type..... 0x100b000
Supported Cards:
    Card Index (CID)..... 3
    Model Identifier..... PCM8024
```

The following table describes the fields in the example.

Field	Description
Switch Type	This field displays the 32-bit numeric switch type for the supported switch.
Model Identifier	This field displays the model identifier for the supported switch type.

Field	Description
Switch Description	This field displays the description for the supported switch type.

show switch

Use the **show switch** command in User EXEC mode to display information about all units in the stack. Use the **show switch** [*unit*] command to display the information about a specific unit on the stack.

Syntax

show switch [*unit*]

- unit* — The unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays stack status information for the switch.

```
console>show switch 1
Switch..... 1
Management Status..... Management Switch
Admin Management Preference..... 4
Switch Type..... 0x73950001
Preconfigured Model Identifier.... PCM8024
Plugged-in Model Identifier..... PCM8024
```

```

Switch Status..... OK
Switch Description..... PCM8024
Expected Code Type..... 0x100b000
Detected Code Version..... I.12.21.1
Detected Code in Flash..... I.12.21.1
Boot Code Version..... I.12.1
Up Time..... 1 days 0 hrs 16
mins 37 secs

```

The following table describes the fields in the example.

Unit	Description
Switch	This field displays the unit identifier assigned to the switch.
Management Status	This field indicates whether the switch is the Management Switch, a stack member, or the status is unassigned.
Admin Management Preference	This field indicates the administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the Management Switch.
Switch Type	This field displays the 32-bit numeric switch type.
Model Identifier	This field displays the model identifier for this switch. Model Identifier is a 32-character field assigned by the switch manufacturer to identify the switch.
Switch Status	This field displays the switch status. Possible values are OK, Unsupported, Code Mismatch, Config Mismatch, or Not Present.
Switch Description	This field displays the switch description.
Expected Code Version	This field indicates the expected code version.

Unit	Description
Detected Code Version	This field displays the version of code running on this switch. If the switch is not present and the data is from preconfiguration, the code version is "None."
Detected Code in Flash	This field displays the version of code that is currently stored in FLASH memory on the switch. This code will execute after the switch is reset. If the switch is not present and the data is from pre-configuration, then the code version is "None."
Boot Code Version	This field displays the version of the boot strapping code.
Up Time	This field displays the system up time.

This example displays information about all units in the stack.

```
console>show switch
```

Switch	Management Status	Preconfig Model ID	Plugged-in Model ID	Switch Status	Code Version

1	Mgmt Switch	PCM8024	PCM8024		1.0.0.0

Different fields in the display are explained as follows:

Unit	Description
Switch	This field displays the unit identifier assigned to the switch.
Management Status	This field indicates whether the switch is the Management Switch, a stack member, or the status is unassigned.
Preconfigured Model Identifier	This field displays the model identifier of a preconfigured switch ready to join the stack. The Model Identifier is a 32-character field assigned by the switch manufacturer to identify the switch.

Unit	Description
Plugged-In Model Identifier	This field displays the model identifier of the switch in the stack. Model Identifier is a 32-character field assigned by the switch manufacturer to identify the switch.
Switch Status	This field indicates the switch status. Possible values for this state are: OK, Unsupported, CodeMismatch, ConfigMismatch, or NotPresent
Code Version	This field indicates the detected version of code on this switch.

Status Parameters for NSF

The **show switch** command is used to display which unit is the management unit and which is the backup unit. Global Status Parameters for NSF are explained as follows:

Parameter	Description	Range	Default
NSF Administrative Status	Whether nonstop forwarding is administratively enabled or disabled	Enabled Disabled	Enabled
NSF Operational Status	Indicates whether NSF is enabled on the stack.	Enabled Disabled	None

Parameter	Description	Range	Default
Last Startup Reason	The type of activation that caused the software to start the last time. There are four options. “Power-On” means that the switch rebooted. This could have been caused by a power cycle or an administrative “Reload” command. “Administrative Move” means that the administrator issued a command for the stand-by manager to take over. “Warm-Auto-Restart” means that the primary management card restarted due to a failure, and the system executed a nonstop forwarding failover. “Cold-Auto-Restart” means that the system switched from the active manager to the backup manager and was unable to maintain user data traffic. This is usually caused by multiple failures occurring close together.	Power-On Administrative-Move Warm-Auto-Restart Cold-Auto-Restart	None
Time Since Last Restart	Time since the current management card became the active management card. For the backup manager, the value is set to 0d 00:00:00	Time Stamp	0d 00:00:00
Restart in progress	Whether a restart is in progress. A restart is not considered complete until all hardware tables have been fully reconciled.	Yes or No	
Warm Restart Ready	Whether the initial full checkpoint has finished	Yes or No	
Status	Whether the running configuration on the backup unit includes all changes made on the management unit.	Current or Stale	

Parameter	Description	Range	Default
Time Since Last Copy	When the running configuration was last copied from the management unit to the backup unit.	Time Stamp	
Time Until Next Copy	The number of seconds until the running configuration will be copied to the backup unit. This line only appears when the running configuration on the backup unit is Stale.	0 - L7_UNITMGR_CONFIG_COPY_HOLDDOWN	

(nsf-stack) #show nsf

Administrative Status..... Enable
Operational Status..... Enable
Last Startup Reason..... Warm Auto-Restart
Time Since Last Restart..... 0 days 16 hrs 52 mins 55 secs
Restart In Progress..... No
Warm Restart Ready..... Yes

Copy of Running Configuration to Backup Unit:
Status..... Stale
Time Since Last Copy..... 0 days 4 hrs 53 mins 22 secs
Time Until Next Copy..... 28 seconds

Unit	NSF Support
----	-----
1	Yes
2	Yes
3	Yes

Per Unit Status Parameters are explained as follows:

Parameter	Description	Range	Default
NSF Support	Whether a unit supports NSF	Yes or No	

show system

Use the **show system** command in User EXEC mode command to display system information.

Syntax

`show system [unit]`

- *unit* — The unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays system information.

```
console#show system
```

```
System Description: Dell Ethernet Switch
```

```
System Up Time: 0 days, 00h:02m:14s
```

```
System Contact:
```

```
System Name:
```

```
System Location:
```

Burned In MAC Address: 00FF.F2A3.8888
System Object ID: 1.3.6.1.4.1.674.10895.3011
System Model ID: PCT6248
Machine Type: Dell 48 Port Gigabit Ethernet
Temperature Sensors:

Unit	Temperature (Celsius)	Status
----	-----	-----
1	25	OK

Fans:

Unit	Description	Status
----	-----	-----
1	Fan 1	OK
1	Fan 2	OK
1	Fan 3	OK
1	Fan 4	OK

Power Supplies:

Unit	Description	Status	Source
----	-----	-----	-----
1	Main	OK	AC
1	Secondary	Failure	DC

show system id

Use the `show system id` command in User EXEC mode to display the system identity information.

Syntax

`show system id [unit]`

- *unit* — The unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

The tag information is on a switch by switch basis.

Example

The following example displays the system service tag information.

```
console>show system id
```

```
Service Tag: 89788978
```

```
Serial number: 8936589782
```

```
Asset tag: 7843678957
```

Unit	Service tag	Serial number	Asset tag
-----	-----	-----	-----
1	89788978	8936589782	7843678957
2	4254675	3216523877	5621987728

show tech-support

Use the **show tech-support** command to display system and configuration information for use in debugging or contacting technical support. The output of the show tech-support command combines the output of the following commands:

- show version
- show sysinfo
- show port all
- show isdp neighbors
- show logging
- show event log
- show logging buffered
- show running config
- show debugging

Syntax

show tech-support

Parameter Ranges

Not applicable

Command Mode

Privileged EXEC mode.

Usage Guidelines

Not applicable

Default Value

Not applicable

Example

console#show tech-support

***** Show Version *****

Switch: 2

System Description..... Powerconnect 6248P,
1.23.0.33

VxWorks 6.5

Machine Type..... Powerconnect 6248P

Machine Model..... PCT6248P

Serial Number.....
CN0PK4632829881C0067

FRU Number..... 1

Part Number..... BCM56314

Maintenance Level..... A

Manufacturer..... 0xbc00

Burned In MAC Address..... 00:1E:4F:04:5D:F4

Software Version..... 1.23.0.33

Operating System..... VxWorks 6.5

Network Processing Device..... BCM56314_A0

Additional Packages..... FASTPATH QOS

FASTPATH Multicast

FASTPATH Stacking

FASTPATH Routing

***** Show SysInfo *****

System Location.....

System Contact.....

System Object ID.....
1.3.6.1.4.1.674.10895.3013

```
System Up Time..... 0 days 0 hrs 11
mins 47 secs
10/100 Ethernet/802.3 interface(s)..... 4
Gig Ethernet/802.3 interface(s)..... 1
10Gig Ethernet/802.3 interface(s)..... 0
Virtual Ethernet/802.3 interface(s)..... 0
```

MIBs Supported:

--More-- or (q)uit

Selecting More (m) continues the display of output for the show tech-support command.

show users

Use the **show users** command in Privileged EXEC mode to display information about the active users.

Syntax

show users [long]

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a list of active users and the information about them.

```
console#show users
```

Username	Protocol	Location
-----	-----	-----
Bob	Serial	
John	SSH	172.16.0.1
Robert	HTTP	172.16.0.8
Betty	Telnet	172.16.1.7

show version

Use the **show version** command in User EXEC mode to displays the system version information.

Syntax

```
show version [unit]
```

- *unit* — The unit number.

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays a system version (this version number is only for demonstration purposes).

```
console>show version

Image Descriptions
image1 : default image
image2 :

Images currently available on Flash
-----
unit    image1    image2    current-active    next-active
-----
1       K.3.9.1    0.0.0.0    image1             image1
2       K.3.9.1    0.0.0.0    image1             image1
```

stack

Use the **stack** command in Global Configuration mode to set the mode to Stack Global Config.

Syntax

stack

Default Configuration

This command has no default mode.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example sets the mode to Stack Global Config.

```
console (config) #stack
console (config-stack) #
```

stack-port

Use the **stack-port** command in Stack Configuration mode to configure Stack ports as either Stacking ports or as Ethernet ports. This command is used to configure CX-4 ports to be either stacking or Ethernet ports. By default, CX-4 ports are Ethernet ports.

Syntax

```
stack-port <unit>/<port-type> <port-num> {ethernet | stack}
```

Default Configuration

By default, these ports are configured as stacking ports.

Command Mode

Stack Configuration mode

User Guidelines

The **clear config** command will not change the stacking port mode. Only the **stack-port** command can change the operating mode of the stacking port and it only takes effect after a reboot when changing between stacking and Ethernet mode. If this command is used with a CX-4 module, the ports will be forced to Ethernet mode upon reboot.

Example

```
console (config-stack) #stack-port 1/xg3 ethernet
console (config-stack) #
```

standby

Use the **standby** command to configure the standby in the stack. This unit comes up as the master when the stack failover occurs. Use the **no** form of this command to reset to default, in which case, FASTPATH automatically selects a standby from the existing stack units if there no preconfiguration.

Syntax

standby *unit*

- *unit*— Valid unit number in the stack. (Range: 1–12 maximum. The range is limited to the number of units available on the stack.)

Default Configuration

This command has no default configuration.

Command Mode

Stack Global Configuration

User Guidelines

No specific guidelines.

Examples

```
console(config)#stack
```

```
console(config-stack)#standby 2
```

switch priority

Use the **switch priority** command in Global Configuration mode to configure the ability of the switch to become the Management Switch. The switch with the highest priority value is chosen to become the Management Switch if the active Management Switch fails.

Syntax

switch *unit* **priority** *value*

- *unit*— The switch identifier. (Range: 1–12)

- *value* — The priority of one backup switch over another. (Range: 0–12)

Default Configuration

The switch priority defaults to the hardware management preference value of 1.

Command Mode

Global Configuration mode

User Guidelines

Switches that do not have the hardware capability to become the Management Switch are not eligible for management.

Once the priority of a switch has been configured, it cannot be reset to the default. Switch priority is not affected by the "clear config" command.

Example

The following example displays how to configure switch number "1" to have a priority of "2" for becoming the Management Switch.

```
console(config)#switch 1 priority 2
```

switch renumber

Use the **switch renumber** command in Global Configuration mode to change the identifier for a switch in the stack. Upon execution, the switch is configured with the configuration information for the new switch, if any is available. The old switch configuration information is retained; however, the old switch will be *operationally unplugged*.

Syntax

```
switch oldunit renumber newunit
```

- *oldunit* — The current switch identifier. (Range: 1–12)
- *newunit* — The updated value of the switch identifier. (Range: 1–12)

Command Mode

Global Configuration mode

User Guidelines

This command is executed on the Management Switch.

Example

The following example displays how to reconfigure switch number “1” to an identifier of “2.”

```
console(config)#switch 1 renumber 2
```

telnet

Use the **telnet** command in Privileged EXEC mode to log into a host that supports Telnet.

Syntax

telnet {*ip-address* / *hostname*} [*port*] [*keyword1*.....]

- *ip-address* — Valid IP address of the destination host.
- *hostname* — Hostname of the destination host. (Range: 1–158 characters)
- *port* — A decimal TCP port number, or one of the keywords from the port table in the usage guidelines (see "Port Table" on page 1326).
- *keyword* — One or more keywords from the keywords table in the user guidelines (see "Keywords Table" on page 1326).

Default Configuration

port — Telnet port (decimal 23) on the host.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

```
console#telnet 1.1.1.1?
```

Keywords Table

Options	Description
debug	Enable telnet debugging mode.
line	Enable telnet linemode.
localecho	Enable telnet localecho.
<cr>	Press ENTER to execute the command.
<port>	Enter the port number.

Port Table

Keyword	Description	Port Number
bgp	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513

Keyword	Description	Port Number
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

Example

Following is an example of using the **telnet** command to connect to 176.213.10.50.

```
console#telnet 176.213.10.50
```

```
Esc U sends telnet EL
```

traceroute

Use the **traceroute** command in Privileged EXEC mode to discover the IP routes that packets actually take when traveling to their destinations.

You can use **traceroute** command in either of two formats:

- You can specify the IP address and hostname in the command. The **traceroute {ipaddress|hostname}** command sets the parameters to their default values.

- You can enter **tracert** to without specifying the IP address and hostname, and specify values for the traceroute parameters.

Syntax

tracert [**ip** | **ipv6**] *ipaddress* | *hostname* [**initTtl** *initTtl*] [**maxTtl** *maxTtl*] [**maxFail** *maxFail*] [**interval** *interval*] [**count** *count*] [**port** *port*] [**size** *size*]

- *ipaddress* — Valid IP address of the destination host.
- *hostname* — Hostname of the destination host (Range: 1–158 characters).
- *initTtl* — The initial time-to-live (TTL); the maximum number of router hops between the local and remote system (Range: 0–255).
- *maxTtl* — The largest TTL value that can be used (Range: 1–255).
- *maxFail* — Terminate the traceroute after failing to receive a response for this number of consecutive probes (Range: 0–255).
- *interval* — The timeout period. If a response is not received within this period of time, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe, then it sends the next probe immediately. (Range: 1–60 seconds).
- *count* — The number of probes to be sent at each TTL level (Range: 1–10).
- *port* — The destination UDP port of the probe. This should be an unused port on the remote destination system (Range: 1–65535).
- *size* — The size, in bytes, of the payload of the Echo Requests sent (Range: 0–65507 bytes).

Default Configuration

The default count is 3 probes.

The default interval is 3 seconds.

The default size is 0 data bytes.

The default port is 33434.

The default initTtl is 1 hop.

The default maxTtl is 30 hops.

The default maxFail is 5 probes.

Command Mode

Privileged EXEC mode.

User Guidelines

There are no user guidelines for this command.

Examples

The following example discovers the routes that packets will actually take when traveling to the destination specified in the command.

```
console#traceroute 192.168.77.171
```

Tracing route over a maximum of 20 hops

1	192.168.21.1	30 ms	10 ms	10 ms
2	*	*	*	*
3	*	*	*	*
4	*	*	*	*
5	*	*	*	*

The following example uses the iterative process to obtain command parameters, and displays the routes that packets actually take when traveling to their destination.

```
console#traceroute
```

```
traceroute# Enter the ip-address|hostname :  
192.168.77.171
```

```
traceroute# Packet size (default: 40 bytes): 30
```

```
traceroute# Max ttl value (default: 20): 10
```

```
traceroute# Number of probes to send at each level  
(default 3):
```

```
traceroute# Timeout (default: 3 seconds): 6
```

```
traceroute# Source ip-address (default to select best  
interface address):
```

```
traceroute# Type of Service byte (default):
```

Tracing route over a maximum of 20 hops

1	192.168.21.1	30 ms	10 ms	10 ms
2		*	*	*
3		*	*	*
4		*	*	*
5		*	*	*

Telnet Server Commands

This chapter explains the following commands:

- ip telnet server disable
- ip telnet port
- show ip telnet

ip telnet server disable

The `ip telnet server disable` command is used to enable/disable the Telnet service on the switch.

Syntax

`ip telnet server disable`
`no ip telnet server disable`

Parameter Ranges

Not applicable

Command Mode

Global Configuration

Usage Guidelines

No specific guidelines.

Default Value

This feature is enabled by default.

Example

```
console#configure
console(config)#ip telnet server disable
console(config)# no ip telnet server disable
```

ip telnet port

The `ip telnet port` command is used to configure the Telnet service port number on the switch.

Syntax

`ip telnet port port number`

- *port number* — Telnet service port number (Range: 1–65535)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration

Usage Guidelines

No specific guidelines.

Example

```
console(config)#ip telnet port 45  
console(config)#no ip telnet port
```

show ip telnet

The `show ip telnet` command displays the status of the Telnet server and the Telnet service port number.

Syntax

```
show ip telnet
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC

Example

```
(console)#show ip telnet  
Telnet Server is Enabled. Port:23
```


User Interface Commands

This chapter explains the following commands:

- enable
- end
- exit
- quit

enable

Use the **enable** command in User EXEC mode to enter the Privileged EXEC mode.

Syntax

enable

Default Configuration

The default privilege level is 15.

Command Mode

User EXEC mode

User Guidelines

If there is no authentication method defined for **enable**, then a level 1 user is not allowed to execute this command.

Example

The following example shows how to enter privileged mode.

```
console>enable
```

```
console#
```

end

Use the **end** command to get the CLI user control back to the privileged execution mode or user execution mode.

Syntax Description

end

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

No specific guidelines.

Example

```
console (config) #end  
console#end  
console>
```

exit

Use the **exit** command to go to the next lower command prompt.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

All command modes except User EXEC

User Guidelines

There are no user guidelines for this command.

Example

The following example changes the configuration mode from Interface Configuration mode to User EXEC mode.

```
console(config-if-1/g1)# exit
console(config)# exit
console#exit
console>
```

quit

Use the **quit** command in User EXEC mode to close an active terminal session by logging off the switch.

Syntax

quit

Default Configuration

This command has no default configuration.

Command Mode

User EXEC command mode

User Guidelines

There are no user guidelines for this command.

Example

The following example closes an active terminal session.

```
console>quit
```

Web Server Commands

This chapter explains the following commands:

- common-name
- country
- crypto certificate generate
- crypto certificate import
- crypto certificate request
- duration
- ip http port
- ip http server
- ip https certificate
- ip https port
- ip https server
- key-generate
- location
- organization-unit
- show crypto certificate mycertificate
- show ip http
- show ip https
- state

common-name

Use the **common-name** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the common-name for the switch.

Syntax

common-name *common-name*

- *common-name* — Specifies the fully qualified URL or IP address of the switch. If left unspecified, this parameter defaults to the lowest IP address of the switch (when the certificate is generated). (Range: 1–64)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certification mode

User Guidelines

This command mode is entered using the **crypto certificate request** or **crypto certificate generate** command.

Example

The following example displays how to specify the name of "router.gm.com."

```
console(config-crypto-cert)#common-name router.gm.com
```

country

Use the **country** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the country.

Syntax

country *country*

- *country* — Specifies the country name. (Range: 2 characters)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation or Crypto Certificate Request mode

User Guidelines

This command mode is entered using the **crypto certificate request** or **crypto certificate generate** command.

Example

The following example displays how to specify the country as "us."

```
console(config-crypto-cert)#country us
```

crypto certificate generate

Use the **crypto certificate generate** command in Global Configuration mode to generate a self-signed HTTPS certificate.

Syntax

crypto certificate *number* **generate**

- *number* — Specifies the certificate number. (Range: 1–2)
- **generate** — Regenerates the SSL RSA key.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

This command is not saved in the router switch configuration; however, the certificate and keys generated by this command are saved in the private configuration. This saved information is never displayed to the user or backed up to another switch. If the RSA keys do not exist, the **generate** parameter must be used.

Example

The following example generates a self-signed HTTPS certificate.

```
console(config)#crypto certificate 1 generate
console(config-crypto-cert)#
```

crypto certificate import

Use the **crypto certificate import** command in Global Configuration mode to import a certificate signed by the Certification Authority for HTTPS.

Syntax

crypto certificate *number* **import**

- *number*— Specifies the certificate number. (Range: 1–2)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enter an external certificate (signed by the Certification Authority) to the switch. To end the session, add a period (.) on a separate line after the input, and press ENTER.

The imported certificate must be based on a certificate request created by the **crypto certificate request** privileged EXEC command.

If the public key found in the certificate does not match the switch's SSL RSA key, the command fails.

This command is not saved in the router configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another switch).

Example

The following example imports a certificate signed by the Certification Authority for HTTPS.

```
console(config)#crypto certificate 1 import
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBI
AkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0km
fhcoHSWr
yflFpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYe
BABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4
MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgcls
ZGFwOi8v
L0VByb3h5JTlWU29mdHdhcmU1MjBSb290JTlWQ2VydGlmaWVyLENO
PXNlcnZl
-----END CERTIFICATE-----
Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2005 to 8/9/2005
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

crypto certificate request

Use the **crypto certificate request** command in Privileged EXEC mode to generate and display a certificate request for HTTPS. This command takes you to Crypto Certificate Request mode.

Syntax

crypto certificate *number* **request**

- *number* — Specifies the certificate number. (Range: 1–2)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, you must first generate a self-signed certificate using the **crypto certificate generate** command in Global Configuration mode in order to generate the keys. Make sure to re-enter values in the certificate fields.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** command in Global Configuration mode to import the certificate into the switch. This certificate replaces the self-signed certificate.

Example

The following example generates and displays a certificate request for HTTPS.

```
console#crypto certificate 1 request
console(config-crypto-cert)#
```


duration

Use the **duration** command in Crypto Certificate Generation mode to specify the duration.

Syntax

duration *days*

- *days* — Specifies the number of days a certification would be valid. If left unspecified, the parameter defaults to 365 days. (Range: 30–3650 days)

Default Configuration

This command defaults to 365 days.

Command Mode

Crypto Certificate Generation mode

User Guidelines

This command mode is entered using the **crypto certificate generate** command.

Example

The following example displays how specify a duration of 50 days that a certification is valid.

```
console (config-crypto-cert) #duration 50
```

ip http port

Use the **ip http port** command in Global Configuration mode to specify the TCP port for use by a web browser to configure the switch. To use the default TCP port, use the **no** form of this command.

Syntax

ip http port *port-number*

no ip http port

- *port-number* — Port number for use by the HTTP server. (Range: 1–65535)

Default Configuration

This default port number is 80.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines. However, specifying 0 as the port number effectively disables HTTP access to the switch.

Example

The following example shows how the http port number is configured to 100.

```
console(config)#ip http port 100
```

ip http server

Use the **ip http server** command in Global Configuration mode to enable the switch to be configured, monitored, or modified from a browser. To disable this function use the **no** form of this command.

Syntax

ip http server

no ip http server

Default Configuration

The default mode is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example enables the switch to be configured from a browser.

```
console(config)#ip http server
```

ip https certificate

Use the **ip https certificate** command in Global Configuration mode to configure the active certificate for HTTPS. To return to the default setting, use the **no** form of this command.

Syntax

ip https certificate *number*

no ip https certificate

- *number*— Specifies the certificate number. (Range: 1–2)

Default Configuration

The default value of the certificate number is 1.

Command Mode

Global Configuration mode

User Guidelines

The HTTPS certificate is generated using the **crypto certificate generate** command in Global Configuration mode.

Example

The following example configures the active certificate for HTTPS.

```
console(config)#ip https certificate 1
```

ip https port

Use the **ip https port** command in Global Configuration mode to configure a TCP port for use by a secure web browser to configure the switch. To use the default port, use the **no** form of this command.

Syntax

`ip https port port-number`

`no ip https port`

- *port-number* — Port number for use by the secure HTTP server. (Range: 1–65535)

Default Configuration

This default port number is 443.

Command Mode

Global Configuration mode

User Guidelines

This command has no user guidelines.

Example

The following example configures the https port number to 100.

```
console(config)#ip https port 100
```

ip https server

Use the `ip https server` command in Global Configuration mode to enable the switch to be configured, monitored, or modified securely from a browser. To disable this function, use the `no` form of this command.

Syntax

`ip https server`

`no ip https server`

Default Configuration

The default for the switch is disabled.

Command Mode

Global Configuration mode

User Guidelines

You must use the **crypto certificate generate** command to generate the HTTPS certificate.

Example

The following example enables the switch to be configured from a browser.

```
console(config)#ip https server
```

key-generate

Use the **key-generate** command in Crypto Certificate Generation mode to specify the key-generate.

Syntax

key-generate [*length*]

- *length* — Specifies the length of the SSL RSA key. If left unspecified, this parameter defaults to 1024. (Range: 512–2048)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation mode

User Guidelines

This command mode is entered using the **crypto certificate request** command.

Example

The following example displays how to specify that you want to regenerate the SSL RSA key 1024 bytes in length.

```
console(config-crypto-cert)#key-generate 1024
```

location

Use the **location** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the location or city name.

Syntax

location *location*

- *location* — Specifies the location or city name. (Range: 1–64 characters)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation or Crypto Certificate Request mode

User Guidelines

This command mode is entered using the **crypto certificate request** or **crypto certificate generate** command.

Example

The following example displays how to specify the city location of "austin."

```
console(config-crypto-cert)#location austin
```

organization-unit

Use the **organization-unit** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the organization unit.

Syntax

organization-unit *organization-unit*

- *organization-unit* — Specifies the organization-unit or department name. (Range: 1–64 characters)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation or Crypto Certificate Request mode

User Guidelines

This command mode is entered using the `crypto certificate request` or `crypto certificate generate` command.

Example

The following example displays how to specify the "generalmotors" organization-unit.

```
console(config-crypto-cert)#organization-unit  
generalmotors
```

show crypto certificate mycertificate

Use the `show crypto certificate mycertificate` command in Privileged EXEC mode to view the SSL certificates of your switch.

Syntax

`show crypto certificate mycertificate [number]`

- **number** — Specifies the certificate number. (Range: 1–2 digits)

Default configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

Example

The following example displays the SSL certificate of a sample switch.

```
console#show crypto certificate mycertificate 1  
-----BEGIN CERTIFICATE-----  
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBI  
AkeAp4HS
```

NnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0km
fhcoHSWr

yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYe
BABDAEEw

CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFaf4
MT9BRD47

ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgcls
ZGFwOi8v

L0VByb3h5JTIwU29mdHdhcmUlmjBSb290JTIwQ2VydGlmWVYLENO
PXNlcnZl

-----END CERTIFICATE-----

Issued by: www.verisign.com

Valid from: 8/9/2003 to 8/9/2004

Subject: CN= router.gm.com, O= General Motors, C= US

Finger print: DC789788 DC88A988 127897BC BB789788

show ip http

Use the **show ip http** command in Privileged EXEC mode to display the HTTP server configuration.

Syntax

show ip http

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC command

User Guidelines

This command has no user guidelines.

Example

The following example displays the HTTP server configuration.

```
console#show ip http
HTTP server enabled. Port: 80
```

show ip https

Use the **show ip https** command in Privileged EXEC mode to display the HTTPS server configuration.

Syntax

```
show ip https
```

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command has no user guidelines.

Example

The following example displays an HTTPS server configuration with DH Key exchange enabled.

```
console#show ip https
HTTPS server enabled. Port: 443
DH Key exchange enabled.
Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
```

Finger print: DC789788 DC88A988 127897BC BB789788

Certificate 2 is inactive

Issued by: self-signed

Valid from: 8/9/2003 to 8/9/2004

Subject: CN= router.gm.com, O= General Motors, C= US

Finger print: 1873B936 88DC3411 BC8932EF 782134BA

The following example displays the HTTPS server configuration with DH Key exchange disabled.

```
console#show ip https
```

HTTPS server enabled. Port: 443

DH Key exchange disabled, parameters are being generated.

Certificate 1 is active

Issued by: www.verisign.com

Valid from: 8/9/2003 to 8/9/2004

Subject: CN= router.gm.com, O= General Motors, C= US

Finger print: DC789788 DC88A988 127897BC BB789788

Certificate 2 is inactive

Issued by: self-signed

Valid from: 8/9/2003 to 8/9/2004

Subject: CN= router.gm.com, O= General Motors, C= US

Finger print: 1873B936 88DC3411 BC8932EF 782134BA

state

Use the **state** command in Crypto Certificate Generation or Crypto Certificate Request mode to specify the state or province name.

Syntax

state *state*

- *state* — Specifies the state or province name. (Range: 1–64 characters)

Default Configuration

This command has no default configuration.

Command Mode

Crypto Certificate Generation or Crypto Certificate Request mode

User Guidelines

This command mode is entered using the **crypto certificate request** or **crypto certificate generate** command.

Example

The following example shows how to specify the state of "texas."

```
console(config-crypto-cert)#state texas
```

